AVG Email Server Edition 2011

User Manual

Document revision 2011.03 (23. 2. 2011)

Copyright AVG Technologies CZ, s.r.o. All rights reserved.
All other trademarks are the property of their respective owners.

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.
This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).
This product uses compression library zlib, Copyright (c) 1995-2002 Jean-loup Gailly and Mark Adler.

Contents

1. Introduction 4

2. AVG Installation Requirements 5

2.1 Operation Systems Supported 5
2.2 Email Servers Supported 5
2.3 Hardware Requirements 5
2.4 Uninstall Previous Versions 5
2.5 MS Exchange Service Packs 6

3. AVG Installation Process 7

3.1 Installation Launch 7
3.2 Activate Your License 8
3.3 Select Installation Type 9
3.4 Custom Install - Custom Options 10
3.5 Installation Completion 11

4. E-mail Scanner for MS Exchange Server 2007/2010 13

4.1 Overview 13
4.2 E-mail Scanner for MS Exchange (routing TA) 16
4.3 E-mail Scanner for MS Exchange (SMTP TA) 17
4.4 E-mail Scanner for MS Exchange (VSAPI) 18
4.5 Technical Notice 20
4.6 Detection Actions 22
4.7 Mail Filtering 23

5. E-mail Scanner for MS Exchange Server 2003 25

5.1 Overview 25
5.2 E-mail Scanner for MS Exchange (VSAPI) 28
5.3 Detection Actions 31
5.4 Mail Filtering 32

6. AVG for Kerio MailServer 33

6.1 Configuration 33
6.1.1 Antivirus 33
6.1.2 Attachment Filter 33

7. Anti-Spam Configuration 38

AVG Email Server Edition 2011 © 2011 Copyright AVG Technologies CZ, s.r.o. All rights reserved.

7.1 Anti-Spam Interface 38
7.2 Anti-Spam Principles 40
7.3 Anti-Spam Settings 40
7.3.1 Anti-Spam Training Wizard 40
7.3.2 Select Folder with Messages 40
7.3.3 Message filtering options 40
7.4 Performance 45
7.5 RBL 47
7.6 Whitelist 48
7.7 Blacklist 49
7.8 Advanced Settings 50

8. AVG Settings Manager 51

9. FAQ and Technical Support 54

1. Introduction

This user manual provides comprehensive documentation for **AVG Email Server Edition 2011**.

Congratulations on your purchase of AVG Email Server Edition 2011!

AVG Email Server Edition 2011 is one of a range of award winning AVG products designed to provide you with peace of mind and total security for your server. As with all AVG products **AVG Email Server Edition 2011** has been completely re-designed, from the ground up, to deliver AVG's renowned and accredited security protection in a new, more user friendly and efficient way.

AVG has been designed and developed to protect your computing and networking activity. Enjoy the experience of full protection from AVG.

Note: *This documentation contains description of specific E-mail Server Edition features. Should you require information about other AVG features, please consult the user guide to Internet Security edition, which contains all the necessary details. You can download the guide from the http://www.avg.com.*

AVG Email Server Edition 2011 © 2011 Copyright AVG Technologies CZ, s.r.o. All rights reserved.

2. AVG Installation Requirements

2.1. Operation Systems Supported

AVG Email Server Edition 2011 is intended to protect e-mail servers running under the following operating systems:

- Windows 2008 Server Edition (x86 and x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Email Servers Supported

The following e-mail servers are supported:

- MS Exchange 2003 Server version
- MS Exchange 2007 Server version
- MS Exchange 2010 Server version
- AVG for Kerio MailServer – version 6.7.2 and higher

2.3. Hardware Requirements

Minimum hardware requirements for **AVG Email Server Edition 2011** are:

- Intel Pentium CPU 1.5 GHz
- 500 MB of free hard drive space (for installation purposes)
- 512 MB of RAM memory

Recommended hardware requirements for **AVG Email Server Edition 2011** are:

- Intel Pentium CPU 1.8 GHz
- 600 MB of free hard drive space (for installation purposes)
- 512 MB of RAM memory

2.4. Uninstall Previous Versions

If you have an older version of AVG Email Server installed, you will need to uninstall it manually before installing **AVG Email Server Edition 2011**. You must manually perform the uninstallation of the previous version, using the standard windows functionality.

- From the start menu ***Start/Settings/Control Panel/Add or Remove***

Programs select the correct program from the list of installed software. Be careful to select the correct AVG program for uninstallation. You need to uninstall the Email Server Edition before uninstalling the AVG File Server Edition.

- Once you have uninstalled the Email Server Edition, you can proceed to uninstall your previous version of AVG File Server Edition. This can be done easily from the start menu ***Start/All Programs/AVG/Uninstall AVG***

- If you have previously used the AVG 8.x or older version, do not forget to uninstall also individual server plug-ins.

  Note: *It will be necessary to restart the store service during the uninstallation process.*

  Exchange plug-in - run setupes.exe with the /uninstall parameter from the folder where the plug-in was installed.

  e.g. C:\AVG4ES2K\setupes.exe /uninstall

  Lotus Domino/Notes plug-in - run setupln.exe with the /uninstall parameter from folder where the plug-in was installed:

  e.g. C:\AVG4LN\setupln.exe /uninstall

2.5. MS Exchange Service Packs

There is no service pack required for MS Exchange 2003 Server; however, it is recommended to keep your system as up to date with the latest service packs and hotfixes as possible in order to obtain maximal available security.

Service Pack for MS Exchange 2003 Server (optional):

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

At the beginning of the setup, all system libraries versions will be examined. If it is necessary to install newer libraries, the installer will rename the old ones with a .delete extension. They will be deleted after the system restart.

Service Pack for MS Exchange 2007 Server (optional):

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

3. AVG Installation Process

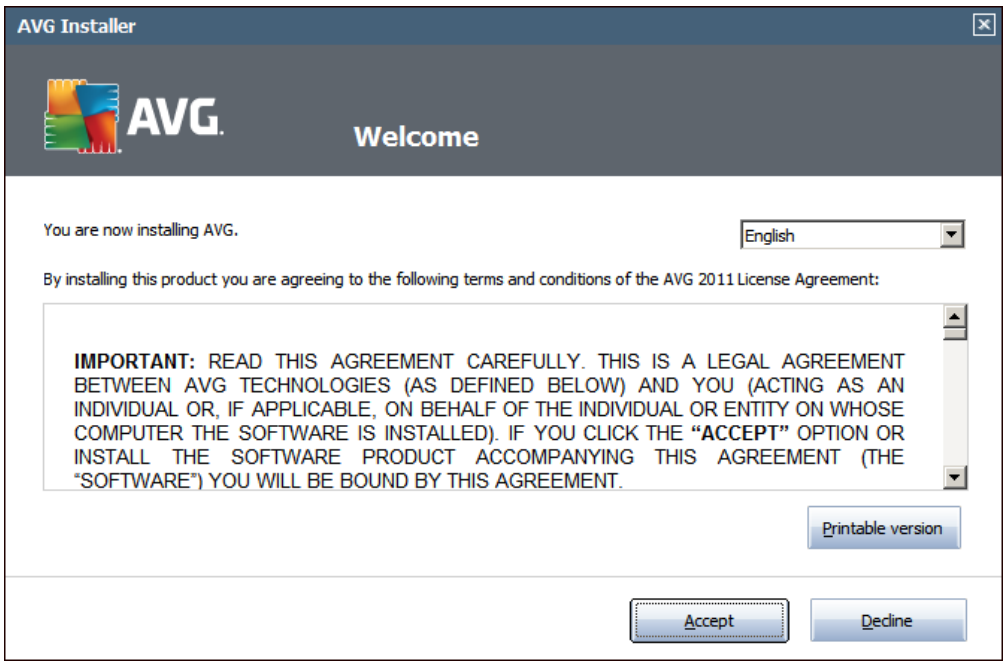
To install AVG on your computer, you need to get the latest installation file. You can use the installation file from the CD that is a part of your box edition but this file might be out-of-date. Therefore we recommended getting the latest installation file online. You can download the file from the AVG website (at http://www.avg.com/download?prd=msw)

Note: *There are two installation packages available for your product - for 32bit operating systems (marked as x86) and for 64bit operating systems (marked as x64). Be sure to use the correct installation package for your specific operating system..*

During the installation process you will be asked for your license number. Please make sure you have it available before starting the installation. The number can be found in the CD packaging. If you purchased your copy of AVG on-line, your license number will have been delivered to you via e-mail.

Once you have downloaded and saved the installation file on your hard drive, you can launch the installation process. The installation is a sequence of dialog windows with a brief description of what do at each step. In the following, we offer an explanation for each dialog window:

3.1. Installation Launch


AVG Installer
AVG
Welcome
You are now installing AVG.
English
By installing this product you are agreeing to the following terms and conditions of the AVG 2011 License Agreement:
IMPORTANT: READ THIS AGREEMENT CAREFULLY. THIS IS A LEGAL AGREEMENT BETWEEN AVG TECHNOLOGIES (AS DEFINED BELOW) AND YOU (ACTING AS AN INDIVIDUAL OR, IF APPLICABLE, ON BEHALF OF THE INDIVIDUAL OR ENTITY ON WHOSE COMPUTER THE SOFTWARE IS INSTALLED). IF YOU CLICK THE "ACCEPT" OPTION OR INSTALL THE SOFTWARE PRODUCT ACCOMPANYING THIS AGREEMENT (THE "SOFTWARE") YOU WILL BE BOUND BY THIS AGREEMENT.
Printable version
Accept
Decline

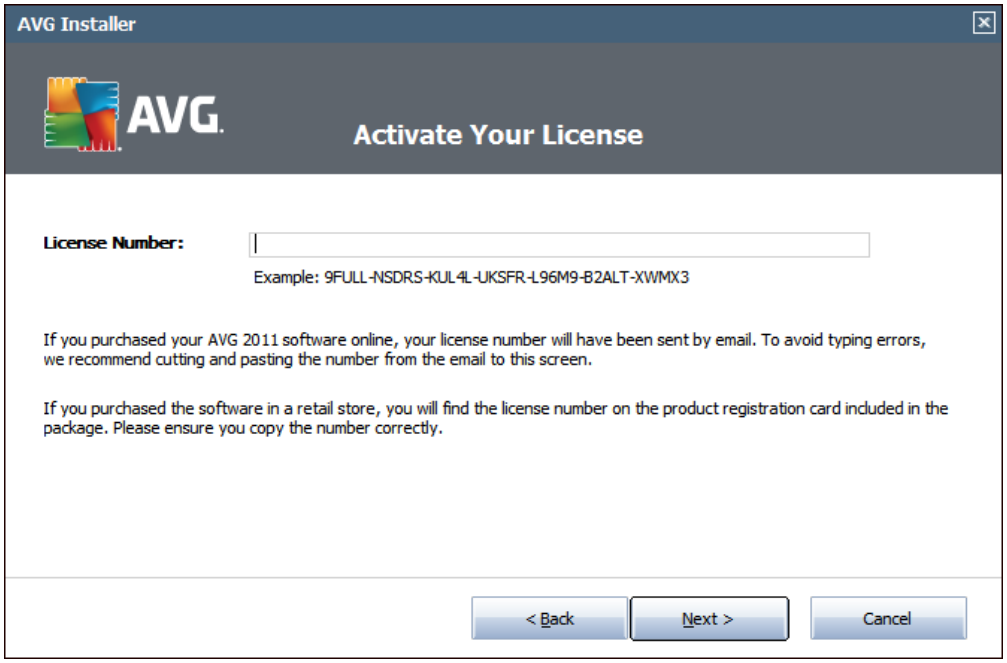
The installation process starts with the ***Welcome*** window. In here you select the language used for the installation process and read the license conditions. Use the ***Printable version*** button to open the license text in a new window. Press the ***Accept*** button to confirm and continue to the next dialog.

Attention: *You will be able to choose also additional languages for the application interface later during the installation process.*

3.2. Activate Your License

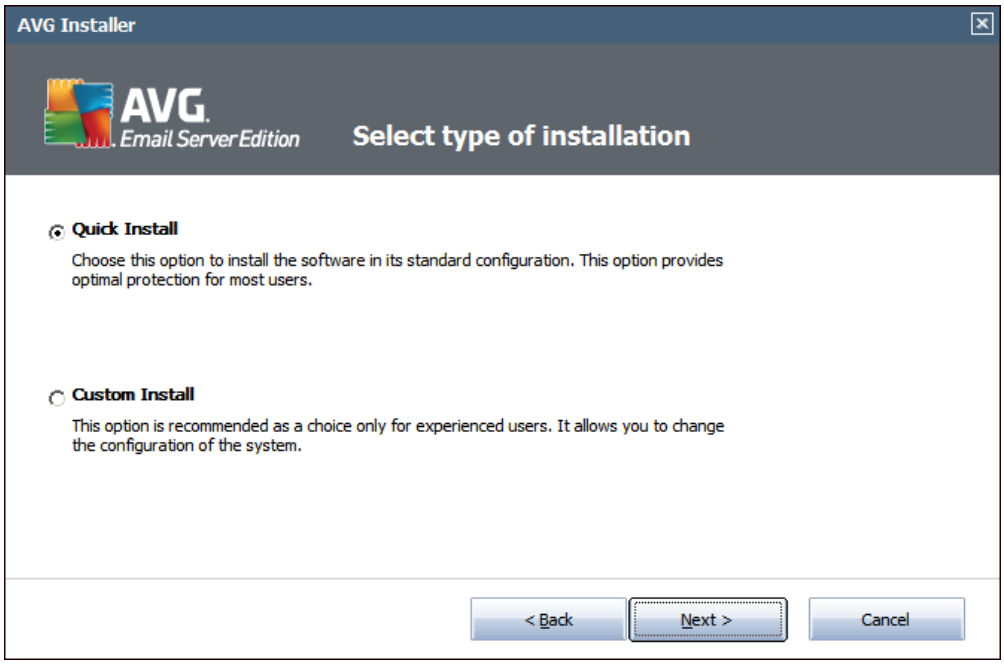
In the ***Activate your License*** dialog you have to fill in your license number.

Enter your license number into the ***License Number*** text field. The license number will be in the confirmation e-mail that you received after purchasing your AVG on-line. You must type in the number exactly as shown. If the digital form of the license number is available (in the email), it is recommended to use the copy and paste method to insert it.


AVG Installer
Activate Your License
License Number:
Example: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX3
If you purchased your AVG 2011 software online, your license number will have been sent by email. To avoid typing errors, we recommend cutting and pasting the number from the email to this screen.
If you purchased the software in a retail store, you will find the license number on the product registration card included in the package. Please ensure you copy the number correctly.
< Back
Next >
Cancel

Press the ***Next*** button to continue the installation process.

3.3. Select Installation Type

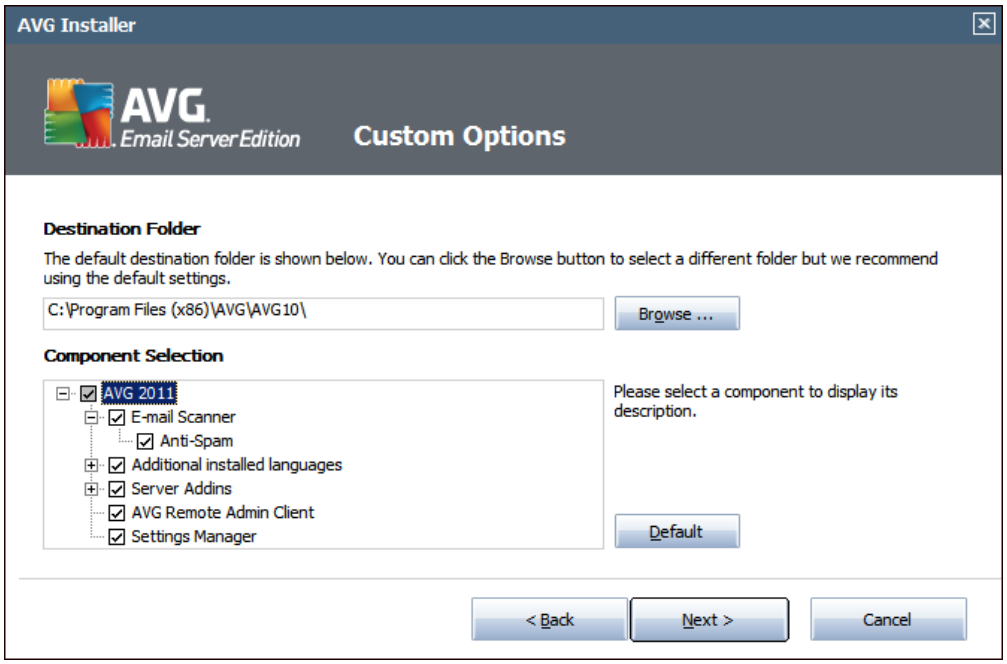

AVG Installer
AVG.
Email Server Edition
Select type of installation
Quick Install
Choose this option to install the software in its standard configuration. This option provides optimal protection for most users.
Custom Install
This option is recommended as a choice only for experienced users. It allows you to change the configuration of the system.
< Back
Next >
Cancel

The ***Select type of Installation*** dialog offers the choice of two installation options: ***Quick Install*** and ***Custom Install***.

For most users, it is highly recommended to keep to the ***Quick Install*** that installs AVG in fully automatic mode with settings predefined by the program vendor. This configuration provides maximum security combined with the optimal use of resources. In the future, if the need arises to change the configuration, you will always have the possibility to do so directly in the AVG application.

Custom Install should only be used by experienced users who have a valid reason to install AVG with non-standard settings. E.g. to fit specific system requirements.

3.4. Custom Install - Custom Options



The ***Destination folder*** dialog allows you to specify the location where AVG should be installed. By default, AVG will be installed to the program files folder located on drive C:. If you want to change this location, use the ***Browse*** button to display the drive structure, and select the respective folder.

The ***Component selection*** section displays an overview of all AVG components that can be installed. If the default settings do not suit you, you can remove/add specific components.

However, you can only select from components that are included in your purchased AVG edition. Only those components will be offered to be installed within the Component Selection dialog!

- ***AVG Remote Admin Client*** - if you intend to connect AVG to an AVG DataCenter (AVG Network Editions), then you need to select this option.

  Note: *Only server components available in the list can be managed remotely!*

- ***Settings Manager*** - a tool suitable mainly for network administrators that allows you to copy, edit and distribute AVG configuration. The configuration can be saved to a portable device (USB flash drive etc.) and then applied manually or any other way to chosen stations.

- ***Additional Installed Languages*** - you can define which language(s) AVG should be installed in. Check the ***Additional installed languages*** item and then select the desired languages from the respective menu.

Basic overview of the individual server components (***Server Addins***):

- ***Anti-Spam Server for MS Exchange***

  Checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods to process each e-mail message, offering maximum possible protection against unwanted e-mail messages.

- ***E-mail Scanner for MS Exchange (routing Transport Agent)***

  Checks all incoming, outgoing and internal e-mail messages going through the MS Exchange HUB role.

  Available for MS Exchange 2007/2010 and can be installed for HUB role only.

- ***E-mail Scanner for MS Exchange (SMTP Transport Agent)***

  Checks all e-mail messages coming through the MS Exchange SMTP interface.

  Available for MS Exchange 2007/2010 only and can be installed for both EDGE and HUB roles.

- ***E-mail Scanner for MS Exchange (VSAPI)***

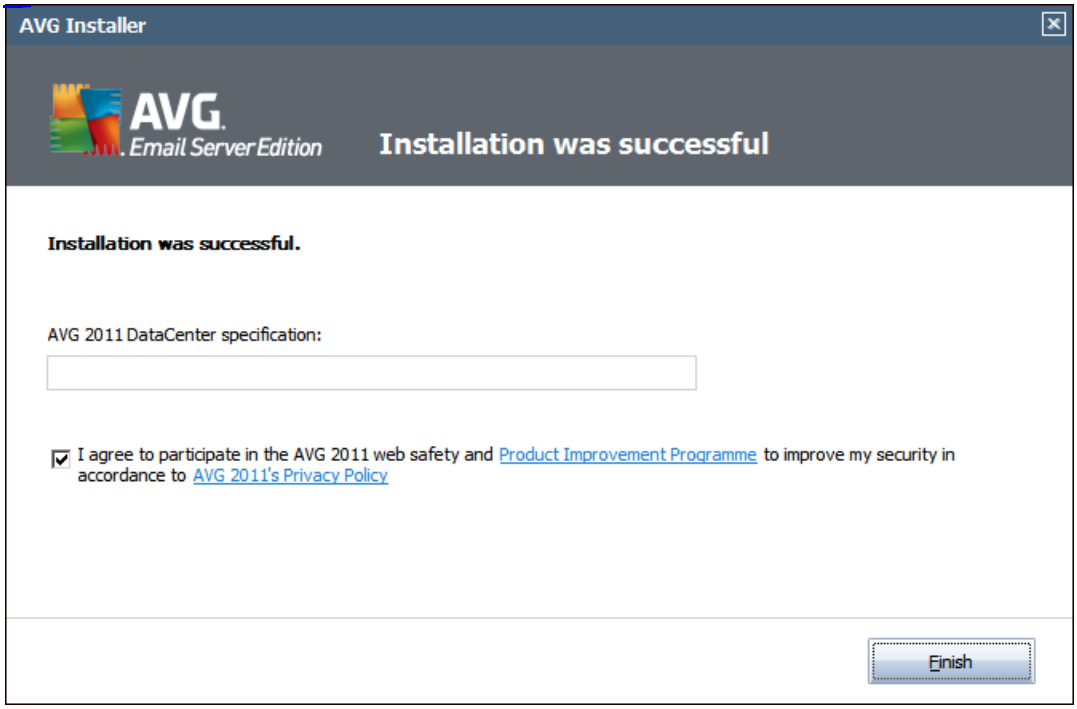
  Checks all e-mail messages stored in user mailboxes. If any viruses are detected, they are moved to the Virus Vault, or completely removed.

Note: *There are different options available for different versions of MS Exchange.*

Continue by pressing the ***Next*** button.

3.5. Installation Completion

If you selected the ***Remote Administration Component*** module during module selection, then the final screen will allow you to define the connection string for connecting to your AVG DataCenter.


AVG Installer
AVG. Email Server Edition
Installation was successful
Installation was successful.
AVG 2011 DataCenter specification:
I agree to participate in the AVG 2011 web safety and Product Improvement Programme to improve my security in accordance to AVG 2011's Privacy Policy
Finish

AVG is now installed on your computer and fully functional. The program is running in the background in fully automatic mode.

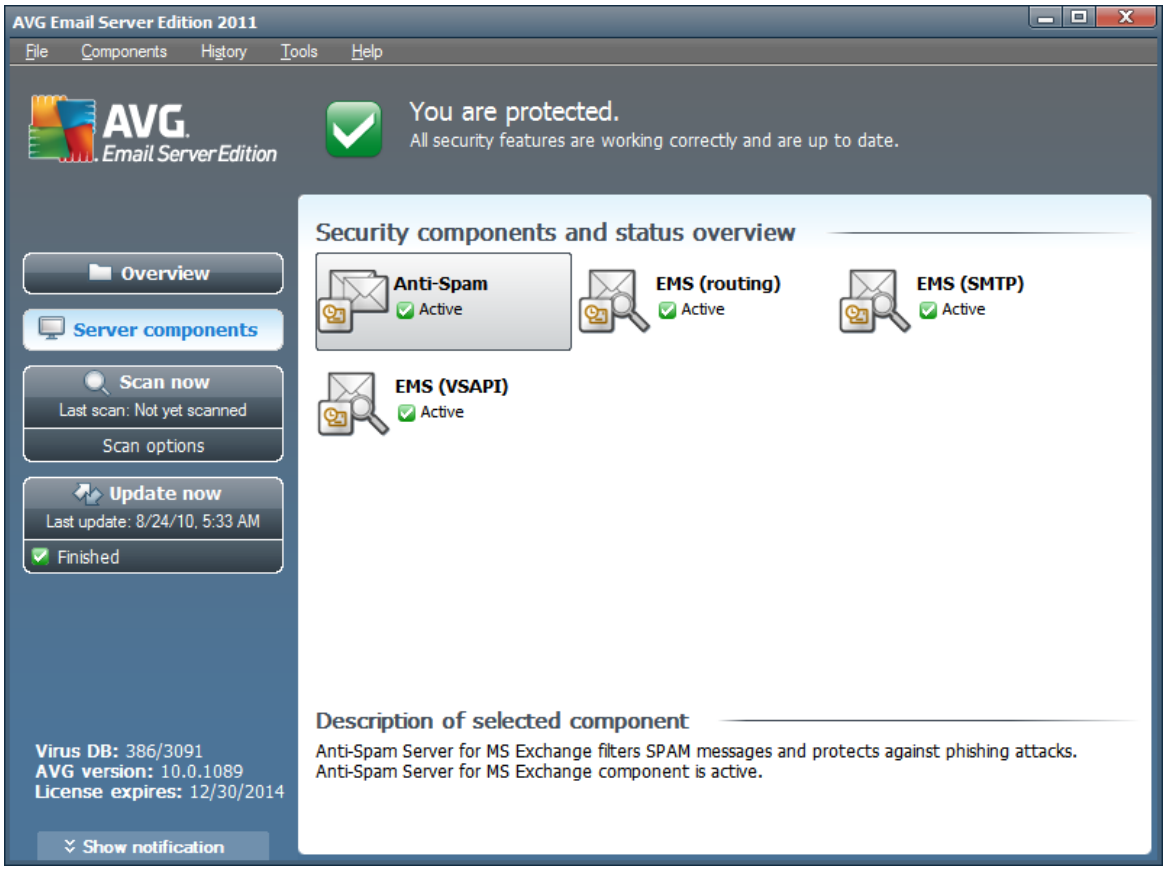
To individually setup protection for your e-mail server, follow the appropriate chapter:

- ***E-mail Scanner for MS Exchange Server 2007/2010***
- ***E-mail Scanner for MS Exchange Server 2003***
- ***AVG for Kerio MailServer***

4. E-mail Scanner for MS Exchange Server 2007/2010

4.1. Overview

The AVG for MS Exchange Server 2007/2010 configuration options are fully integrated within the AVG Email Server Edition 2011 as server components.



Basic overview of the individual server components:

- ***Anti-Spam - Anti-Spam Server for MS Exchange***

  Checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods to process each e-mail message, offering maximum possible protection against unwanted e-mail messages.

- ***EMS (routing) - E-mail Scanner for MS Exchange (routing Transport Agent)***

  Checks all incoming, outgoing and internal e-mail messages going through the MS Exchange HUB role.

  Available for MS Exchange 2007/2010 and can be installed for HUB role only.

- ***EMS (SMTP) - E-mail Scanner for MS Exchange (SMTP Transport Agent)***

  Checks all e-mail messages coming through the MS Exchange SMTP interface.

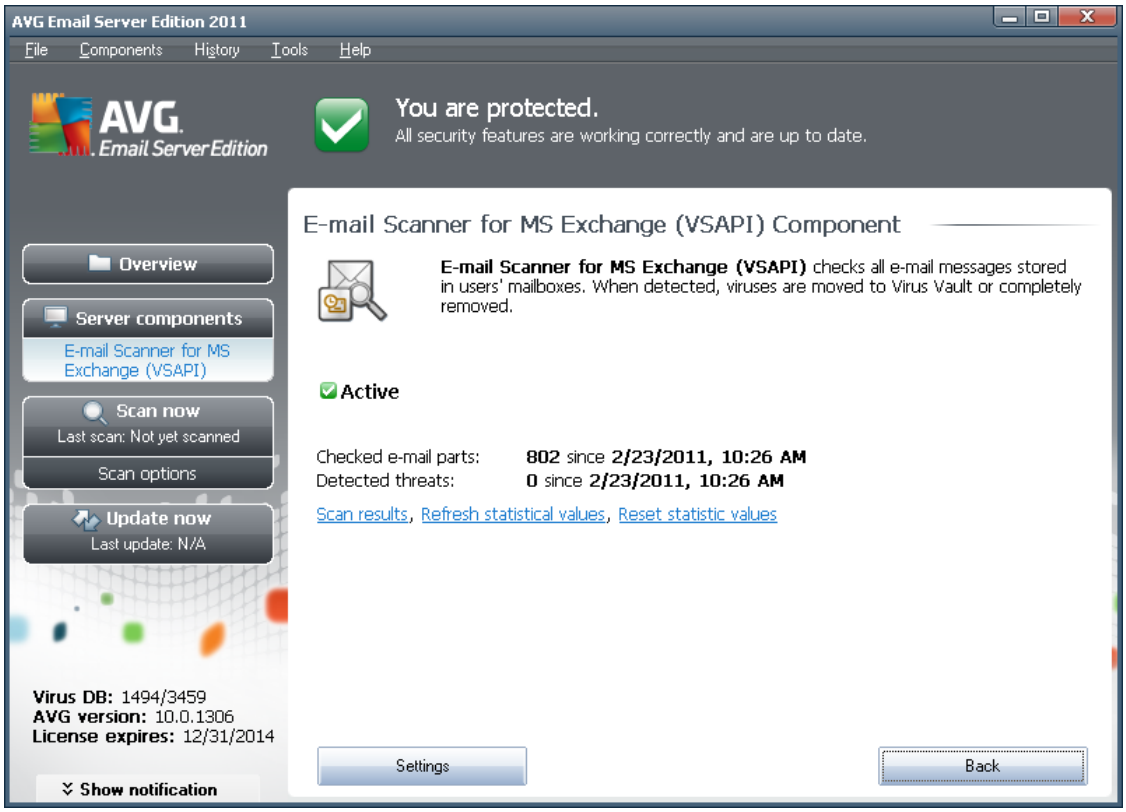
  Available for MS Exchange 2007/2010 only and can be installed for both EDGE and HUB roles.

- ***EMS (VSAPI) - E-mail Scanner for MS Exchange (VSAPI)***

  Checks all e-mail messages stored in user mailboxes. If any viruses are detected, they are moved to the Virus Vault, or completely removed.

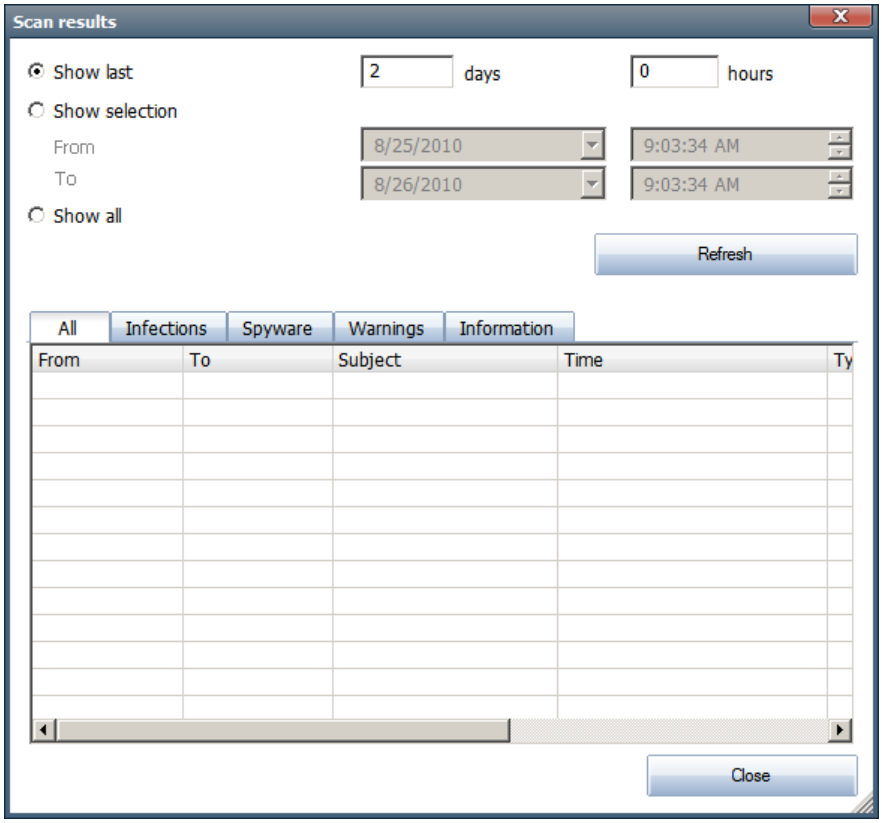
Important note: *If you decided to install and use VSAPI in combination with routing Transport agent on a Hub Exchange role, your e-mail messages will be scanned twice. To avoid this, please review the* ***Technical notice*** *chapter below for more details.*

Double-click a required component to open its interface. With the exception of Anti-Spam, all the components share the following common control buttons and links:


AVG Email Server Edition 2011
File
Components
History
Tools
Help
AVG
Email Server Edition
You are protected.
All security features are working correctly and are up to date.
Overview
Server components
E-mail Scanner for MS Exchange (VSAPI)
Scan now
Last scan: Not yet scanned
Scan options
Update now
Last update: N/A
Virus DB: 1494/3459
AVG version: 10.0.1306
License expires: 12/31/2014
Show notification
E-mail Scanner for MS Exchange (VSAPI) Component
E-mail Scanner for MS Exchange (VSAPI) checks all e-mail messages stored in users' mailboxes. When detected, viruses are moved to Virus Vault or completely removed.
Active
Checked e-mail parts: 802 since 2/23/2011, 10:26 AM
Detected threats: 0 since 2/23/2011, 10:26 AM
Scan results, Refresh statistical values, Reset statistic values
Settings
Back

- ***Scan Results***

  Opens a new dialog where you can review scan results:



Here you can check messages divided into several tabs according to their severity. See configuration of individual components for amending the severity and reporting.

By default there are displayed only results for the last two days. You can change the displayed period by amending the following options:

- o ***Show last*** - insert preferred days and hours.
- o ***Show selection*** - choose a custom time and date interval.
- o ***Show all*** - Displays results for the whole time period.

Use ***Refresh*** button to reload the results.

- ***Refresh statistical values*** - updates stats displayed above.
- ***Reset statistical values*** - resets all the stats to zero.

The working buttons are as follows:

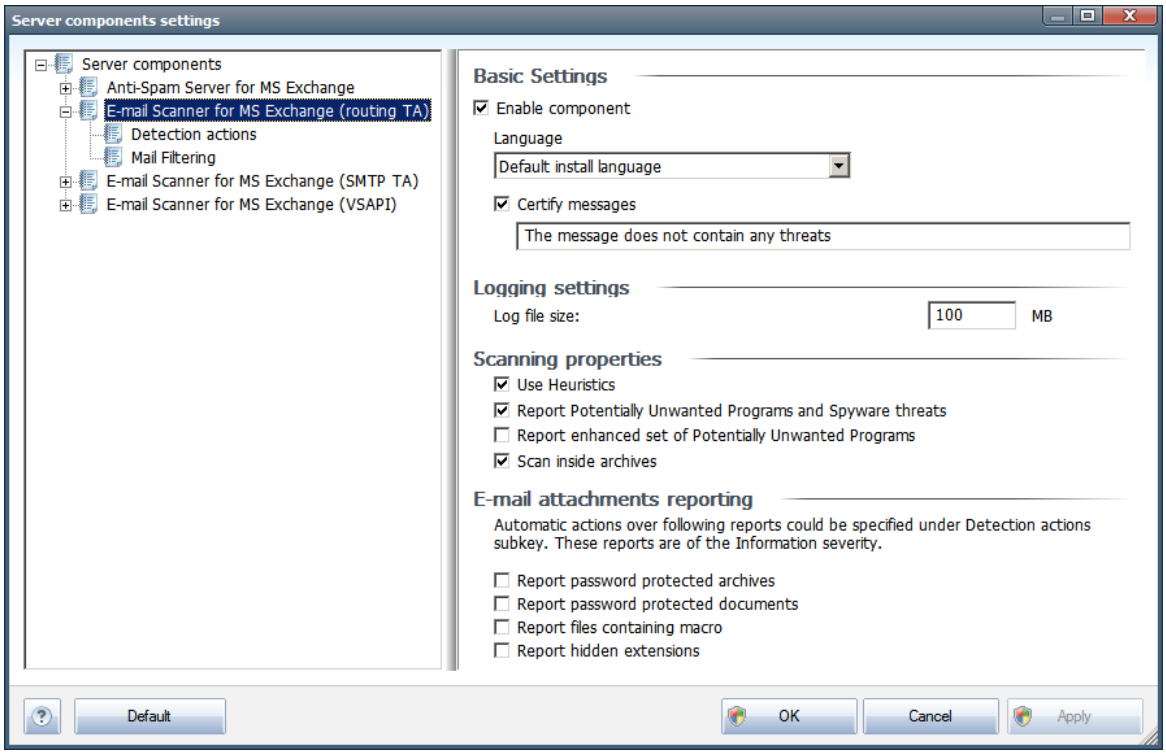
- ***Settings*** - use this button to open settings of the component.
- ***Back*** - press this button to return to the Server components overview.

You will find more information on individual settings of all components in the chapters below.

4.2. E-mail Scanner for MS Exchange (routing TA)

To open the settings of ***E-mail Scanner for MS Exchange (routing transport agent)*** , select the ***Settings*** button from the interface of the component.

From the ***Server components*** list select the ***E-mail Scanner for MS Exchange (routing TA)*** item:



The ***Basic Settings*** section contains the following options:

- ***Enable component*** - uncheck to disable the whole component.
- ***Language*** - select preferred component language.
- ***Certify messages*** - check this if you wish to add a certification note to all scanned messages. You can customize the message in the next field.

The ***Logging settings*** section:

- ***Log file size*** - choose a preferred size of the log file. Default value: 100 MB.

The ***Scanning properties*** section:

- ***Use Heuristics*** - check this box to enable heuristic analysis method during

scanning.

- ***Report Potentially Unwanted Programs and Spyware threats*** - check this option to report the presence of potentially unwanted programs and spyware.

- ***Report enhanced set of Potentially Unwanted Programs*** - check to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later, or programs that always harmless but might be unwanted (various toolbars etc.). This is an additional measure that increases your computer security and comfort even more, however it can possibly block legal programs, and is therefore switched off by default. Note: This detection feature is additional to the previous option, so if you want protection from the basic types of spyware, always keep the previous box checked.

- ***Scan inside archives*** - check this option to let the scanner look also inside archived files (zip, rar, etc.)

The ***E-mail attachments reporting*** section allows you to choose which items should be reported during scanning. If checked, each e-mail with such an item will contain [INFORMATION] tag in the message subject. This is the default configuration which can be easily amended in the ***Detection actions section***, part ***Information*** (see below).

The following options are available:

- ***Report password protected archives***

- ***Report password protected documents***

- ***Report files containing macro***

- ***Report hidden extensions***

There are also these sub-items available in the following tree structure:

- ***Detection actions***

- ***Mail filtering***

4.3. E-mail Scanner for MS Exchange (SMTP TA)

The configuration for the ***E-mail Scanner for MS Exchange (SMTP Transport Agent)*** is exactly the same as in the case of routing transport agent. For more information please see the ***E-mail Scanner for MS Exchange (routing TA)*** chapter above.

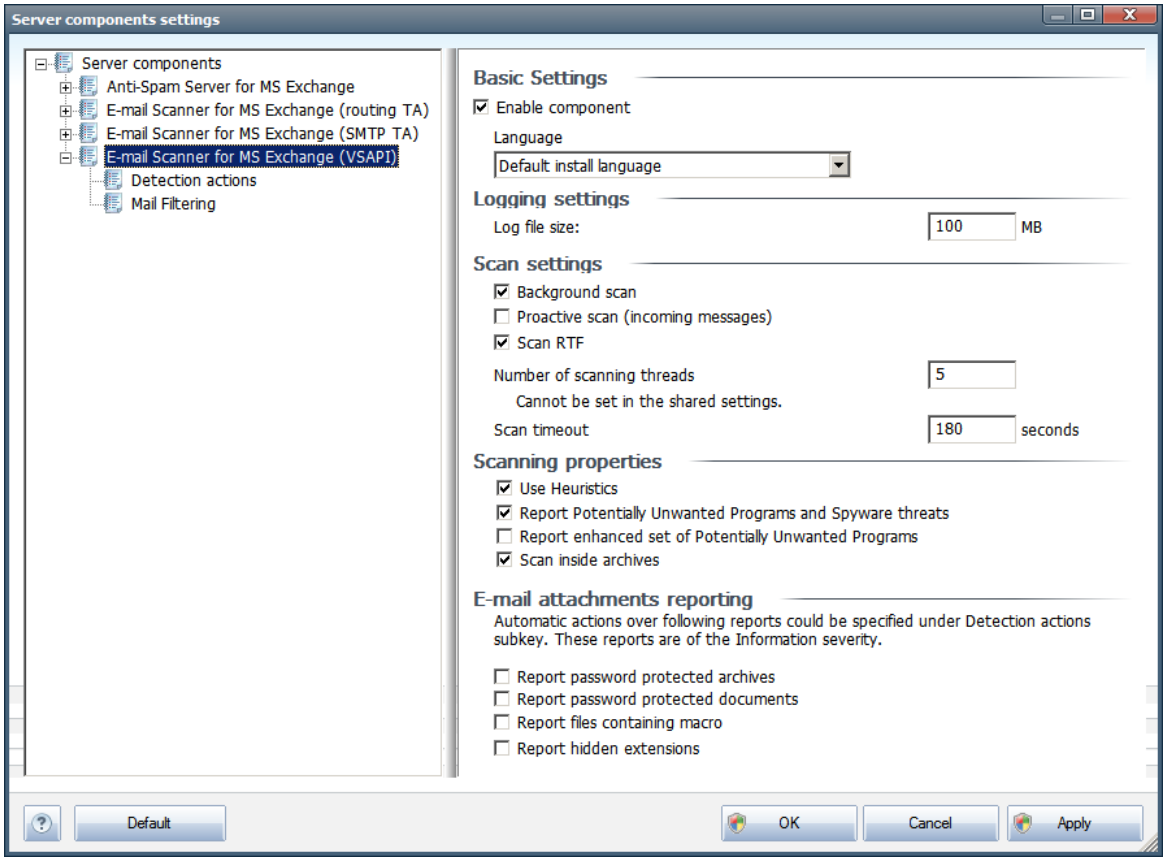
There are also these sub-items available in the following tree structure:

- ***Detection actions***

- ***Mail filtering***

4.4. E-mail Scanner for MS Exchange (VSAPI)

This item contains settings of the ***E-mail Scanner for MS Exchange (VSAPI)***.



The ***Basic Settings*** section contains the following options:

- ***Enable component*** - uncheck to disable the whole component.
- ***Language*** - select preferred component language.

The ***Logging settings*** section:

- ***Log file size*** - choose a preferred size of the log file. Default value: 100 MB.

The ***Scan settings*** section:

- ***Background Scan*** – you can enable or disable the background scanning process here. Background scanning is one of the features of the VSAPI 2.0/2.5 application interface. It provides threaded scanning of the Exchange Messaging Databases. Whenever an item that has not been scanned with the latest AVG virus base update is encountered in the users' mailbox folders, it is submitted to AVG for Exchange Server to be scanned. Scanning and searching for the not examined objects runs in parallel.

A specific low priority thread is used for each database, which guarantees other tasks (e.g. e-mail messages storage in the Microsoft Exchange database) are always carried out preferentially.

- ***Proactive Scan (incoming messages)***

  You can enable or disable the proactive scanning function of VSAPI 2.0/2.5 here. This scanning occurs when an item is delivered to a folder, but a request has not been made by a client.

  As soon as messages are submitted to the Exchange store, they enter the global scanning queue as low priority (maximum of 30 items). They are scanned on the first in, first out (FIFO) basis. If an item is accessed while still in the queue, it is changed to high priority.

  Note: *Overflow messages will continue to the store unscanned.*

Note: *Even if you disable both* ***Background Scan*** *and* ***Proactive Scan*** *options, the on access scanner will be still active when an user will try to download a message with the MS Outlook client.*

- ***Scan RTF*** - you can specify here, whether the RTF file type should be scanned or not.
- ***Number of Scanning Threads*** - the scanning process is threaded by default to increase the overall scanning performance by a certain level of parallelism. You can change the threads count here.

  The default number of threads is computed as 2 times the 'number_of_processors' + 1.

  The minimum number of threads is computed as ('number of processors'+1) divided by 2.

  The maximum number of threads is computed as 'Number of Processors' multiplied by 5 + 1.

  If the value is the minimum or lesser value or the maximum or greater, the default value is used.

- ***Scan Timeout*** - the maximum continuous interval (in seconds) for one thread to access the message that is being scanned (the default value is 180 seconds).

The ***Scanning properties*** section:

- ***Use Heuristics*** - check this box to enable heuristic analysis method during scanning.
- ***Report Potentially Unwanted Programs and Spyware threats*** - check this option to report the presence of potentially unwanted programs and spyware.
- ***Report enhanced set of Potentially Unwanted Programs*** - check to detect extended package of spyware: programs that are perfectly ok and harmless

when acquired from the manufacturer directly, but can be misused for malicious purposes later, or programs that always harmless but might be unwanted (various toolbars etc.). This is an additional measure that increases your computer security and comfort even more, however it can possibly block legal programs, and is therefore switched off by default. Note: This detection feature is additional to the previous option, so if you want protection from the basic types of spyware, always keep the previous box checked.

- ***Scan inside archives*** - check this option to let the scanner look also inside archived files (zip, rar, etc.)

The ***E-mail attachments reporting*** section allows you to choose which items should be reported during scanning. The default configuration can be easily amended in the ***Detection actions section***, part ***Information*** (see below).

The following options are available:

- ***Report password protected archives***
- ***Report password protected documents***
- ***Report files containing macro***
- ***Report hidden extensions***

Generally, some of these features are user extensions of the Microsoft VSAPI 2.0/2.5 application interface services. For the detailed information on the VSAPI 2.0/2.5 please refer to the following links (and also the links accessible from the referenced ones):

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - for information on Exchange and antivirus software interaction
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 for information on additional VSAPI 2.5 features in Exchange 2003 Server application.

There are also these sub-items available in the following tree structure:

- ***Detection actions***
- ***Mail filtering***

4.5. Technical Notice

This information relates to situation when you install and use both VSAPI and routing Transport Agent on a Hub Exchange role. In such case, your e-mail messages will be scanned twice (first by the VSAPI on-access scanner and then by the routing Transport Agent).

Due to the way the VSAPI interface works, there might occur some inconsistencies in scanning results as well as unnecessary load. Therefore, to avoid duplicated scanning,

we recommend a small fix (see below) to resolve this issue instantly.

Note: *Adjusting registry is advised only to experienced users. We recommend that before you edit the registry, you back up the registry and understand how to restore it if a problem occurs.*

Open the Registry editor (Windows menu ***Start/Run***, type in ***regedit*** and press enter). Navigate to the following branch:

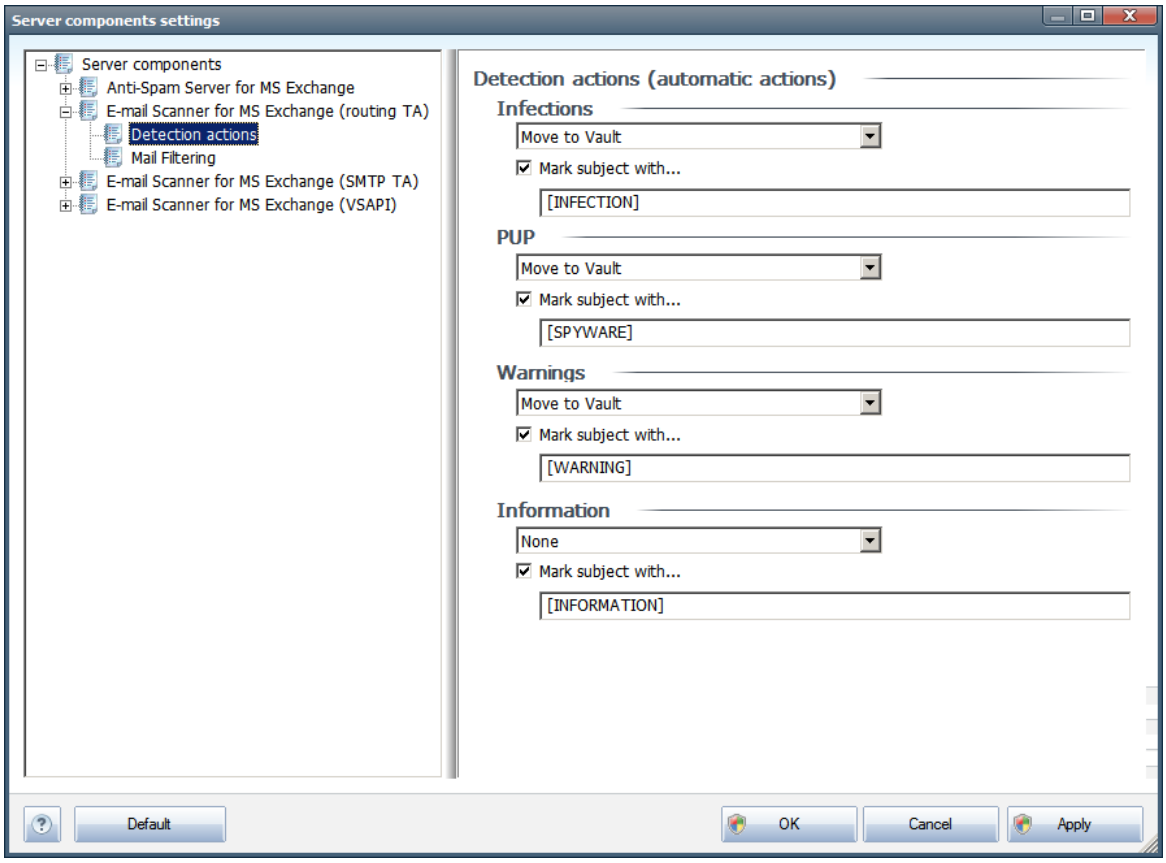
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan

Right-click in the right part of the window and from the context menu select ***New/DWORD (32-bit) value***. Name the new value ***TransportExclusion***. Double click it once created and change its value to ***1***.

And finally, to apply the change to the MS Exchange server, you need to set ***ReloadNow*** value to 1. Do so by double clicking it and changing its value.

This way you will disable the outgoing scanning by VSAPI On-access scanner. The change should be active within a few minutes.

4.6. Detection Actions



In the ***Detection actions*** sub-item you can choose automatic actions that should take place during the scanning process.

The actions are available for the following items:

- ***Infections***
- ***PUP (Potentially Unwanted Programs)***
- ***Warnings***
- ***Information***

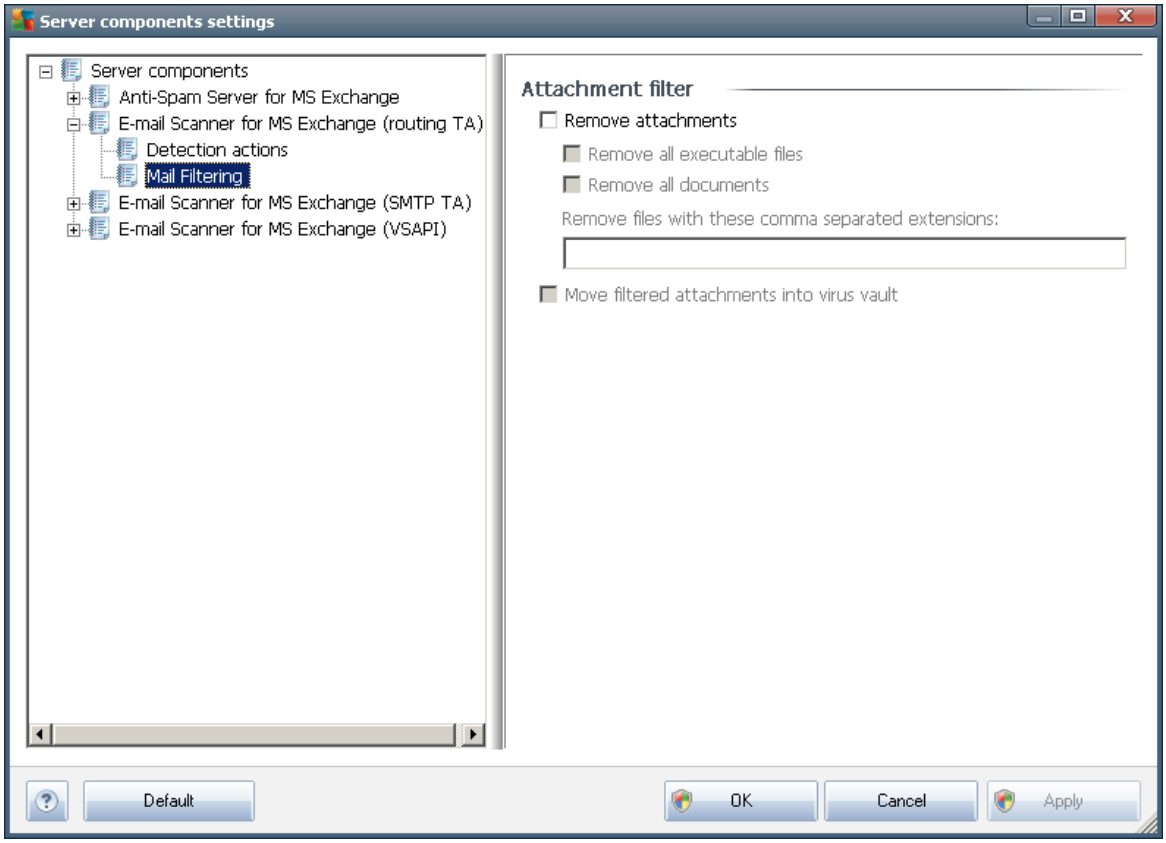
Use the roll-down menu to choose an action for each item:

- ***None*** - no action will be taken.
- ***Move to Vault*** - the given threat will be moved to Virus Vault.
- ***Remove*** - the given threat will be removed.

To select a custom subject text for messages that contain the given item/threat, check the ***Mark subject with...*** box and fill-in a preferred value.

Note: *The last mentioned feature is not available for E-mail Scanner for MS Exchange VSAPI.*

4.7. Mail Filtering



In the ***Mail Filtering*** sub-item you can choose which attachments should be automatically removed, if any. The following options are available:

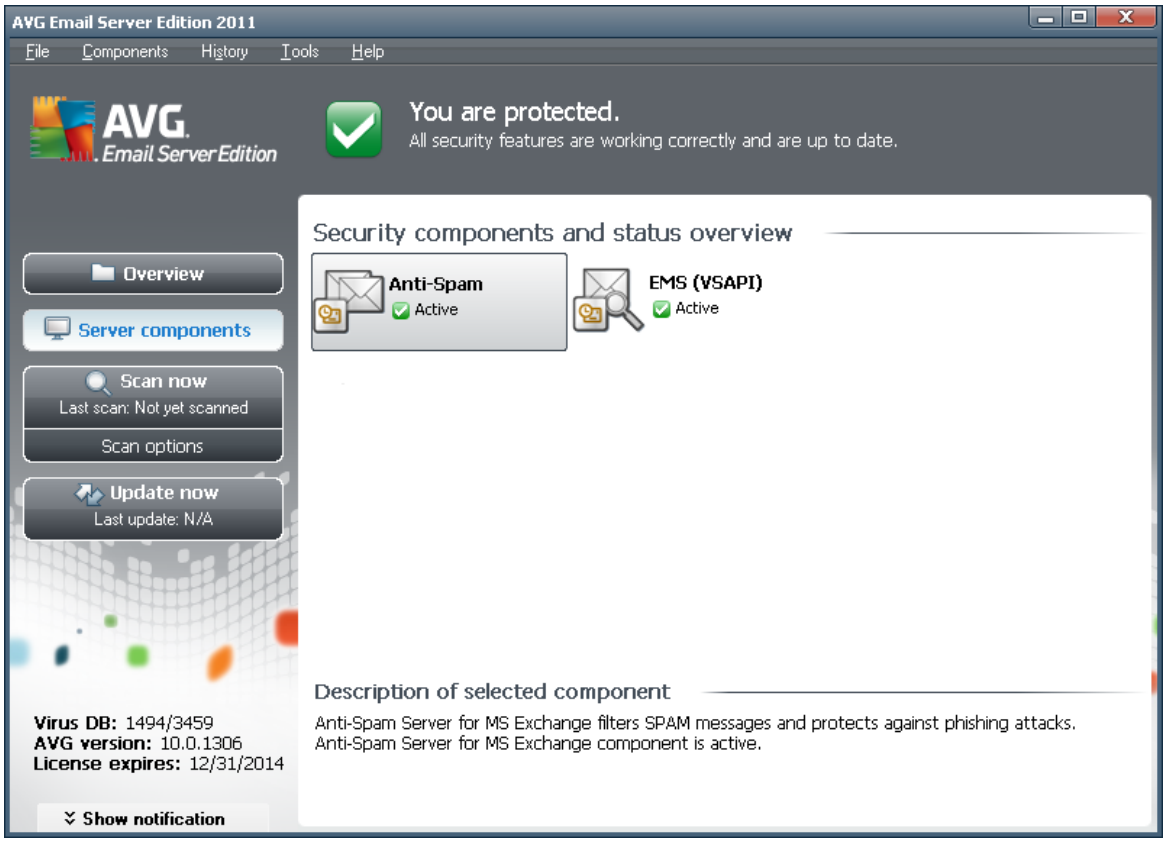
- ***Remove attachments*** - check this box to enable the feature.
- ***Remove all executable files*** - removes all executables.
- ***Remove all documents*** - removes all document files.
- ***Remove files with these comma separated extensions*** - fill the box with file extensions you wish to automatically remove. Separate the extensions with comma.
- ***Move filtered attachments into virus vault*** - check if you don't want the filtered attachments to be removed completely. With this box checked, all attachments chosen in this dialog will be automatically moved into the Virus

Vault quarantine environment. It is a safe place to store potentially malicious files - you can view and examine them without endangering your system. The Virus Vault can be accessed from the upper menu of your **AVG Email Server Edition 2011** main interface. Simply left-click the ***History*** item a choose ***Virus Vault*** item from the context menu.

5. E-mail Scanner for MS Exchange Server 2003

5.1. Overview

The E-mail Scanner for MS Exchange Server 2003 configuration options are fully integrated within the AVG Email Server Edition 2011 as a server component.



The server components include the following:

Basic overview of the individual server components:

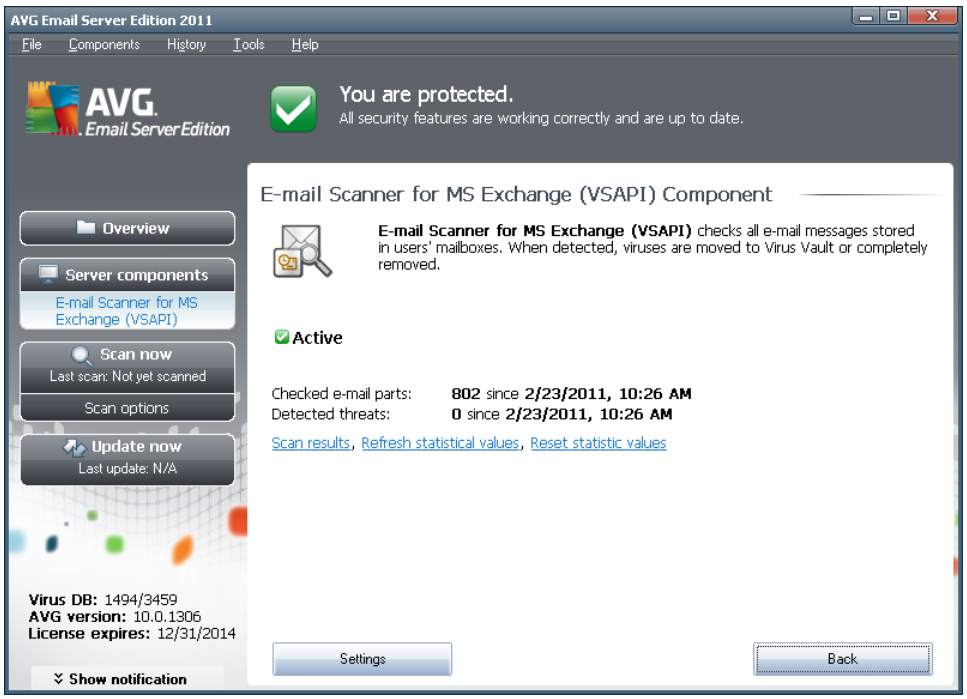
- ***Anti-Spam - Anti-Spam Server for MS Exchange***

  Checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods to process each e-mail message, offering maximum possible protection against unwanted e-mail messages.

- ***EMS (VSAPI) - E-mail Scanner for MS Exchange (VSAPI)***

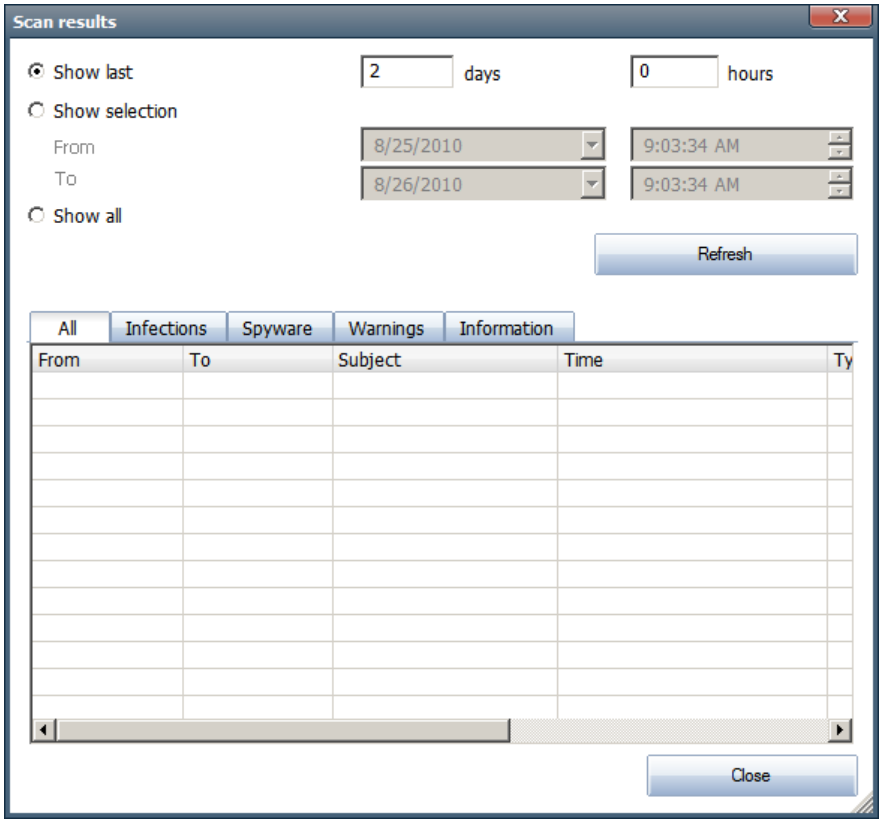
  Checks all e-mail messages stored in user mailboxes. If any viruses are detected, they are moved to the Virus Vault, or completely removed.

Double-click a required component to open its interface. The ***Anti-Spam component*** has its own unique screen described in a separate chapter. The ***E-mail Scanner for MS Exchange (VSAPI)*** interface features the following control buttons and links:


AVG Email Server Edition 2011
File
Components
History
Tools
Help
AVG. Email Server Edition
You are protected.
All security features are working correctly and are up to date.
Overview
Server components
E-mail Scanner for MS Exchange (VSAPI)
Scan now
Last scan: Not yet scanned
Scan options
Update now
Last update: N/A
Virus DB: 1494/3459
AVG version: 10.0.1306
License expires: 12/31/2014
Show notification
E-mail Scanner for MS Exchange (VSAPI) Component
E-mail Scanner for MS Exchange (VSAPI) checks all e-mail messages stored in users' mailboxes. When detected, viruses are moved to Virus Vault or completely removed.
Active
Checked e-mail parts: 802 since 2/23/2011, 10:26 AM
Detected threats: 0 since 2/23/2011, 10:26 AM
Scan results, Refresh statistical values, Reset statistic values
Settings
Back

- ***Scan Results***

  Opens a new dialog where you can review scan results:



Here you can check messages divided into several tabs according to their severity. See configuration of individual components for amending the severity and reporting.

By default there are displayed only results for the last two days. You can change the displayed period by amending the following options:

- ***Show last*** - insert preferred days and hours.
- ***Show selection*** - choose a custom time and date interval.
- ***Show all*** - Displays results for the whole time period.

Use ***Refresh*** button to reload the results.

- ***Refresh statistical values*** - updates stats displayed above.
- ***Reset statistical values*** - resets all the stats to zero.

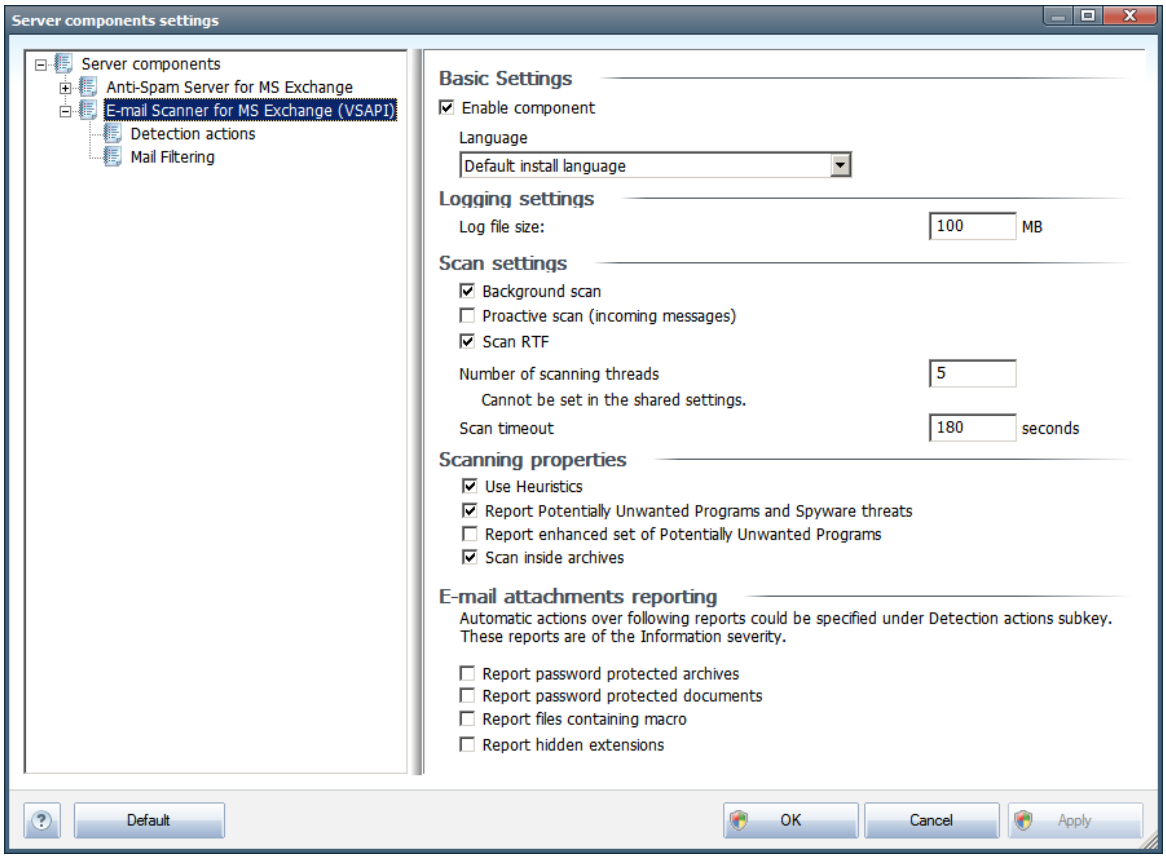
The working buttons are as follows:

- ***Settings*** - use this button to open settings of the component.
- ***Back*** - press this button to return to the Server components overview.

You will find more information on individual settings of all components in the chapters below.

5.2. E-mail Scanner for MS Exchange (VSAPI)

This item contains settings of the ***E-mail Scanner for MS Exchange (VSAPI)***.



The ***Basic Settings*** section contains the following options:

- ***Enable component*** - uncheck to disable the whole component.
- ***Language*** - select preferred component language.

The ***Logging settings*** section:

- ***Log file size*** - choose a preferred size of the log file. Default value: 100 MB.

The ***Scan settings*** section:

- ***Background Scan*** – you can enable or disable the background scanning process here. Background scanning is one of the features of the VSAPI 2.0/2.5 application interface. It provides threaded scanning of the Exchange Messaging Databases. Whenever an item that has not been scanned with the latest AVG

virus base update is encountered in the users' mailbox folders, it is submitted to AVG for Exchange Server to be scanned. Scanning and searching for the not examined objects runs in parallel.

A specific low priority thread is used for each database, which guarantees other tasks (e.g. e-mail messages storage in the Microsoft Exchange database) are always carried out preferentially.

- ***Proactive Scan (incoming messages)***

  You can enable or disable the proactive scanning function of VSAPI 2.0/2.5 here. This scanning occurs when an item is delivered to a folder, but a request has not been made by a client.

  As soon as messages are submitted to the Exchange store, they enter the global scanning queue as low priority (maximum of 30 items). They are scanned on the first in, first out (FIFO) basis. If an item is accessed while still in the queue, it is changed to high priority.

  Note: *Overflow messages will continue to the store unscanned.*

Note: *Even if you disable both* ***Background Scan*** *and* ***Proactive Scan*** *options, the on access scanner will be still active when an user will try to download a message with the MS Outlook client.*

- ***Scan RTF*** - you can specify here, whether the RTF file type should be scanned or not.
- ***Number of Scanning Threads*** - the scanning process is threaded by default to increase the overall scanning performance by a certain level of parallelism. You can change the threads count here.

  The default number of threads is computed as 2 times the 'number_of_processors' + 1.

  The minimum number of threads is computed as ('number of processors'+1) divided by 2.

  The maximum number of threads is computed as 'Number of Processors' multiplied by 5 + 1.

  If the value is the minimum or lesser value or the maximum or greater, the default value is used.

- ***Scan Timeout*** - the maximum continuous interval (in seconds) for one thread to access the message that is being scanned (the default value is 180 seconds).

The ***Scanning properties*** section:

- ***Use Heuristics*** - check this box to enable heuristic analysis method during scanning.
- ***Report Potentially Unwanted Programs and Spyware threats*** - check this

option to report the presence of potentially unwanted programs and spyware.

- ***Report enhanced set of Potentially Unwanted Programs*** - check to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later, or programs that always harmless but might be unwanted (various toolbars etc.). This is an additional measure that increases your computer security and comfort even more, however it can possibly block legal programs, and is therefore switched off by default. Note: This detection feature is additional to the previous option, so if you want protection from the basic types of spyware, always keep the previous box checked.

- ***Scan inside archives*** - check this option to let the scanner look also inside archived files (zip, rar, etc.)

The ***E-mail attachments reporting*** section allows you to choose which items should be reported during scanning. The default configuration can be easily amended in the ***Detection actions section***, part ***Information*** (see below).

The following options are available:

- ***Report password protected archives***

- ***Report password protected documents***

- ***Report files containing macro***

- ***Report hidden extensions***

Generally, all these features are user extensions of the Microsoft VSAPI 2.0/2.5 application interface services. For the detailed information on the VSAPI 2.0/2.5 please refer to the following links (and also the links accessible from the referenced ones):

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - for information on Exchange and antivirus software interaction

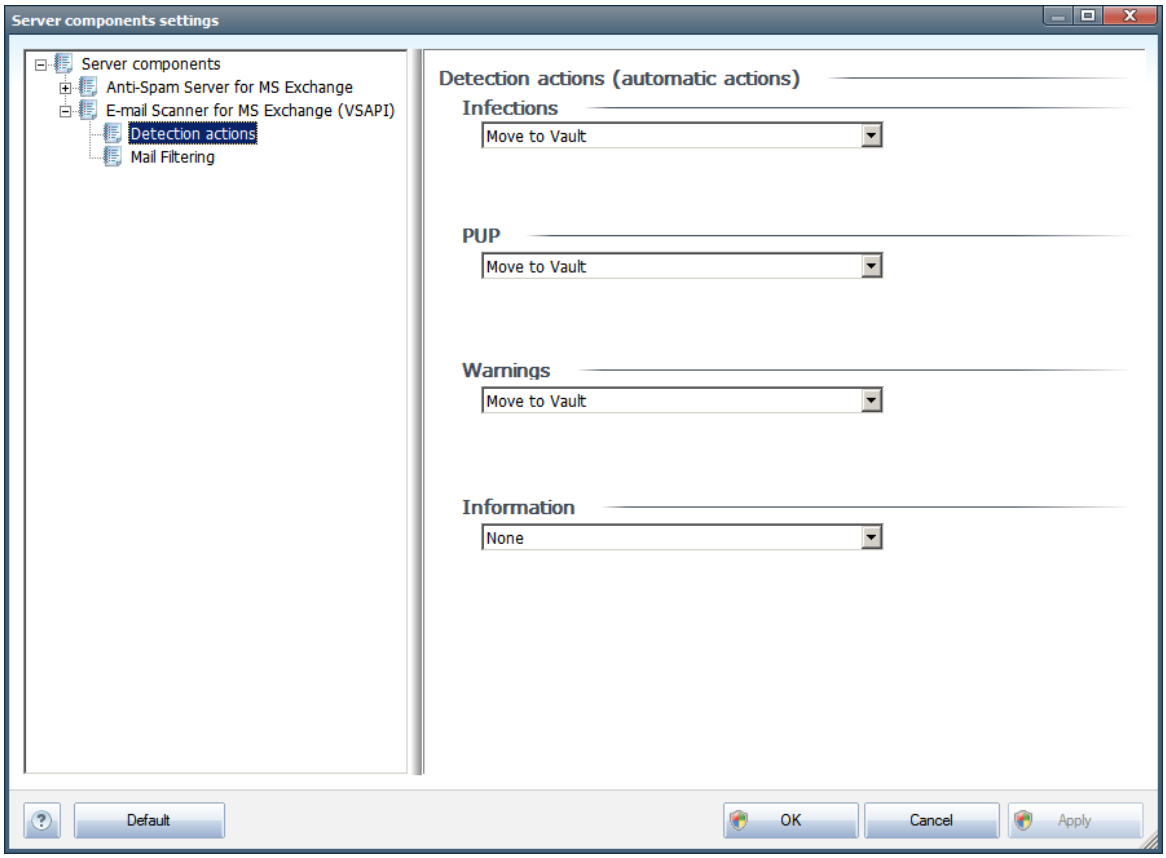
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 for information on additional VSAPI 2.5 features in Exchange 2003 Server application.

There are also these sub-items available in the following tree structure:

- ***Detection actions***

- ***Mail filtering***

5.3. Detection Actions



In the ***Detection actions*** sub-item you can choose automatic actions that should take place during the scanning process.

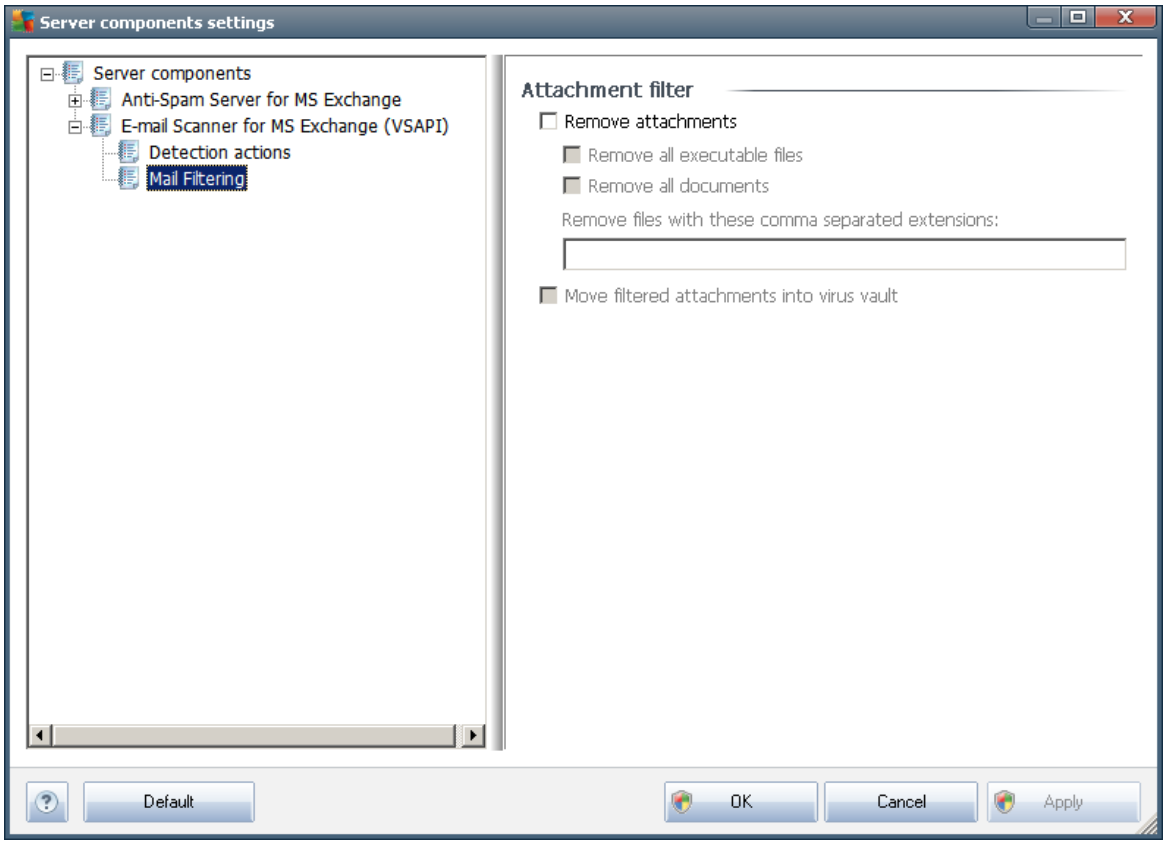
The actions are available for the following items:

- ***Infections***
- ***PUP (Potentially Unwanted Programs)***
- ***Warnings***
- ***Information***

Use the roll-down menu to choose an action for each item:

- ***None*** - no action will be taken.
- ***Move to Vault*** - the given threat will be moved to Virus Vault.
- ***Remove*** - the given threat will be removed.

5.4. Mail Filtering



In the ***Mail Filtering*** sub-item you can choose which attachments should be automatically removed, if any. The following options are available:

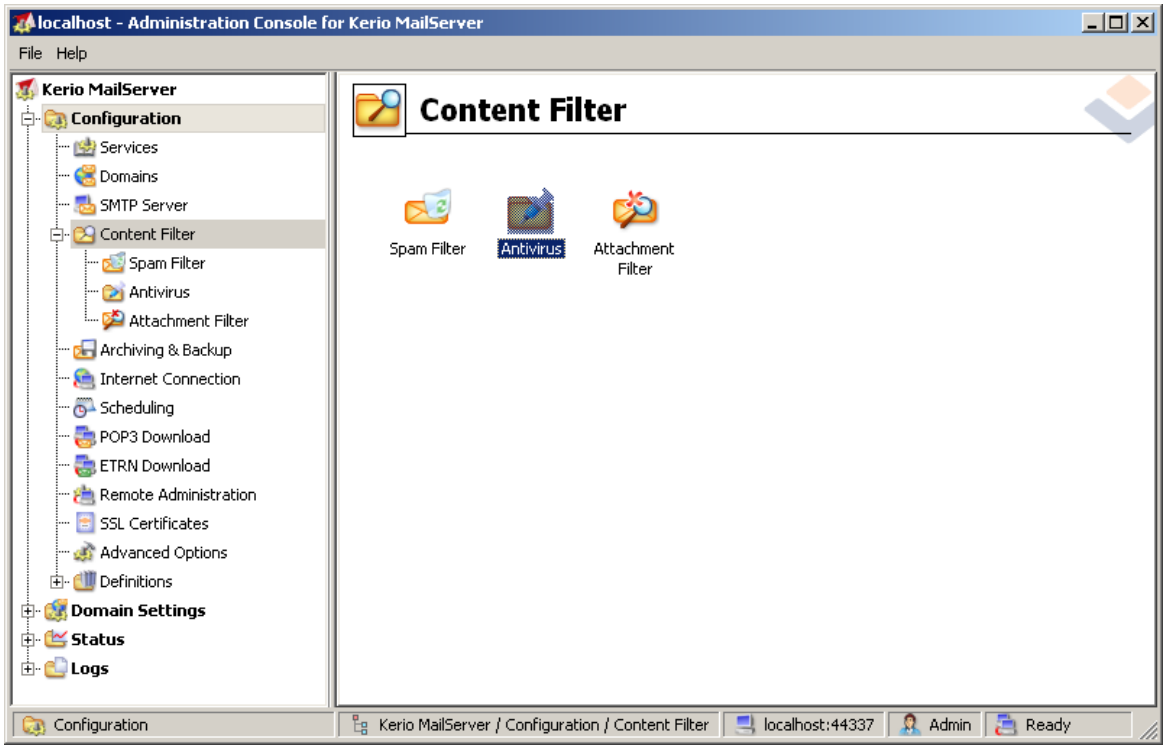
- ***Remove attachments*** - check this box to enable the feature.
- ***Remove all executable files*** - removes all executables.
- ***Remove all documents*** - removes all document files.
- ***Remove files with these comma separated extensions*** - fill the box with file extensions you wish to automatically remove. Separate the extensions with comma.
- ***Move filtered attachments into virus vault*** - check if you don't want the filtered attachments to be removed completely. With this box checked, all attachments chosen in this dialog will be automatically moved into the Virus Vault quarantine environment. It is a safe place to store potentially malicious files - you can access and examine them without endangering your system. The Virus Vault can be accessed from the upper menu of your **AVG Email Server Edition 2011** main interface. Simply left-click the ***History*** item a choose ***Virus Vault*** item from the context menu.

AVG Email Server Edition 2011 © 2011 Copyright AVG Technologies CZ, s.r.o. All rights reserved.

6. AVG for Kerio MailServer

6.1. Configuration

The anti-virus protection mechanism is integrated directly into the Kerio MailServer application. In order to activate e-mail protection of Kerio MailServer by the AVG scanning engine, launch the Kerio Administration Console application. In the control tree on the left side of the application window choose the Content Filter sub-branch in the Configuration branch:

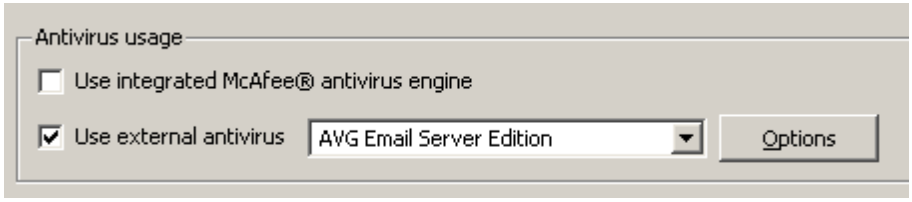


Clicking the Content Filter item will display a dialog with three items:

- ***Spam Filter***
- ***Antivirus*** (see section ***Antivirus***)
- ***Attachment Filter*** (see section ***Attachment Filter***)

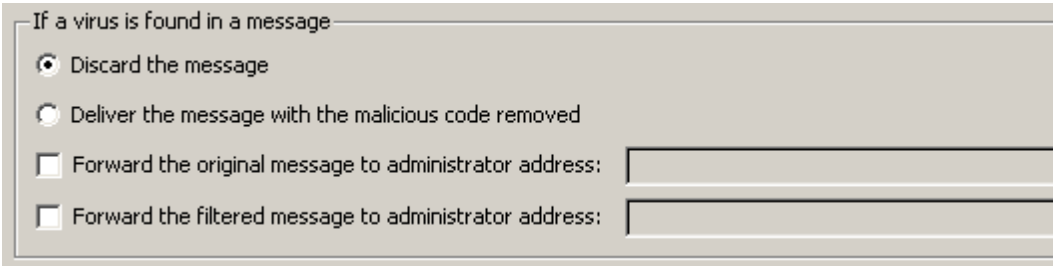
6.1.1. Antivirus

To activate AVG for Kerio MailServer, select the Use external antivirus checkbox and choose the AVG Email Server Edition item from the external software menu in the Antivirus usage frame of the configuration window:



In the following section you can specify what to do with an infected or filtered message:

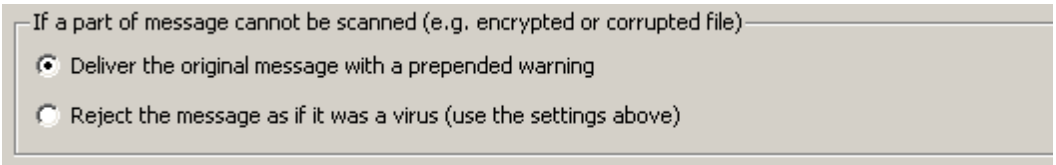
- ***If a virus is found in a message***


If a virus is found in a message
Discard the message
Deliver the message with the malicious code removed
Forward the original message to administrator address:
Forward the filtered message to administrator address:

This frame specifies the action to be carried out when a virus is detected in a message, or when a message is filtered by an attachment filter:

  - ***Discard the message*** – when selected, the infected or filtered message will be deleted.
  - ***Deliver the message with the malicious code removed*** – when selected, the message will be delivered to the recipient, but without the possibly harmful attachment.
  - ***Forward the original message to administrator address*** – when selected, the virus infected message is forwarded to the address specified in the address text field
  - ***Forward the filtered message to administrator address*** - when selected, the filtered message is forwarded to the address specified in the address text field

- ***If a part of message cannot be scanned (e.g. encrypted or corrupted file)***


If a part of message cannot be scanned (e.g. encrypted or corrupted file)
Deliver the original message with a prepended warning
Reject the message as if it was a virus (use the settings above)

This frame specifies the action to be taken when part of the message or attachment cannot be scanned:

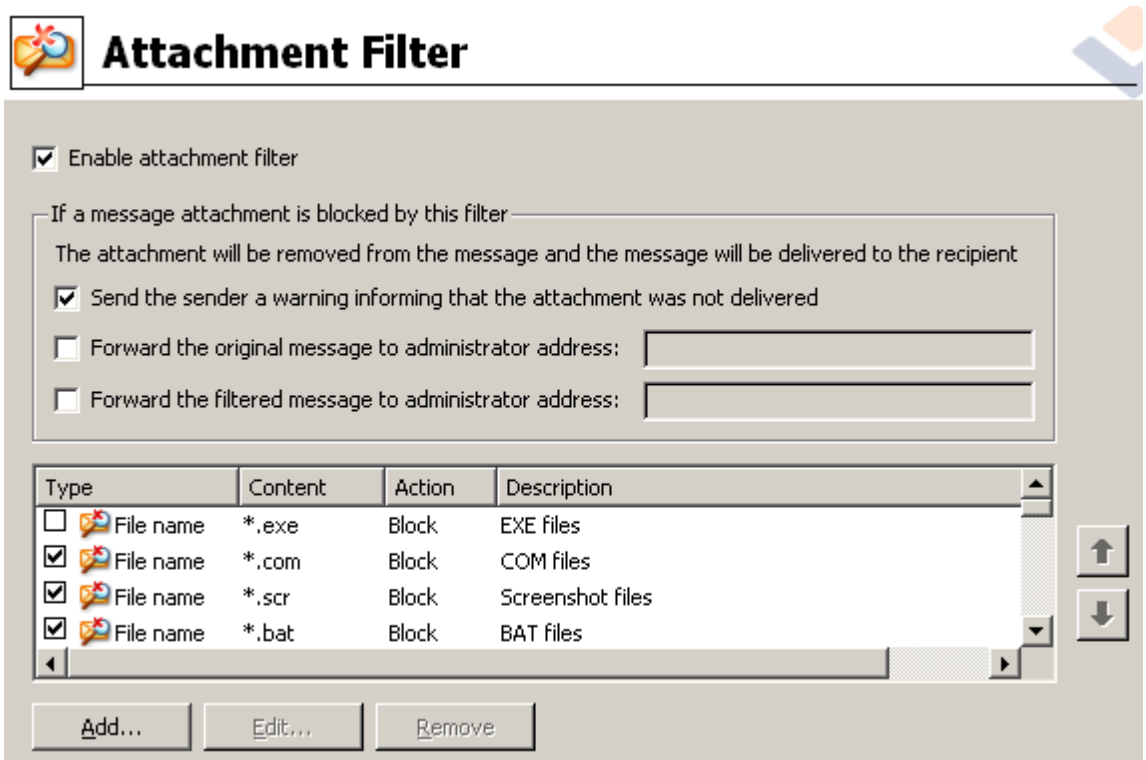
  - ***Deliver the original message with a prepared warning*** — the message

(or attachment) will be delivered unchecked. The user will be warned that the message may still contain viruses.

- ***Reject the message as if it was virus*** — the system will react the same way as when a virus was detected (i.e. the message will be delivered without any attachment or rejected). This option is safe, but sending password protected archives will be virtually impossible.

6.1.2. Attachment Filter

In the Attachment Filter menu there is a list of various attachment definitions:


Attachment Filter
Enable attachment filter
If a message attachment is blocked by this filter
The attachment will be removed from the message and the message will be delivered to the recipient
Send the sender a warning informing that the attachment was not delivered
Forward the original message to administrator address:
Forward the filtered message to administrator address:
Type
Content
Action
Description
File name *.exe Block EXE files
File name *.com Block COM files
File name *.scr Block Screenshot files
File name *.bat Block BAT files
Add...
Edit...
Remove

You can enable/disable filtering of mail attachments by selecting the Enable attachment filter checkbox. Optionally you can change the following settings:

- ***Send a warning to sender that the attachment was not delivered***

  The sender will receive a warning from Kerio MailServer, that he/she has sent a message with a virus or blocked attachment.

- ***Forward the original message to administrator address***

  The message will be forwarded (as it is — with the infected or forbidden attachment) to a defined email address, regardless of whether it is a local or an external address.

- ***Forward the filtered message to administrator address***

The message without its infected or prohibited attachment will be (apart from the actions selected below) forwarded to the specified e-mail address. This can be used to verify the correct functioning of the antivirus and/or attachment filter.

In the list of extensions, each item has four fields:

- ***Type*** – specification of the kind of attachment determined by the extension given in the Content field. Possible types are File name or MIME type. You can select the respective box in this field to include/exclude the item from attachment filtering.
- ***Content*** – an extension to be filtered can be specified here. You can use operation system wildcards here (for example the string '*.doc.*' stands for any file with the .doc extension, and any other extension following).
- ***Action*** – define action to be performed with the particular attachment. Possible actions are Accept (accept the attachment), and Block (an action will be performed as defined above the list of disabled attachments).
- ***Description*** – description of the attachment is defined in this field.

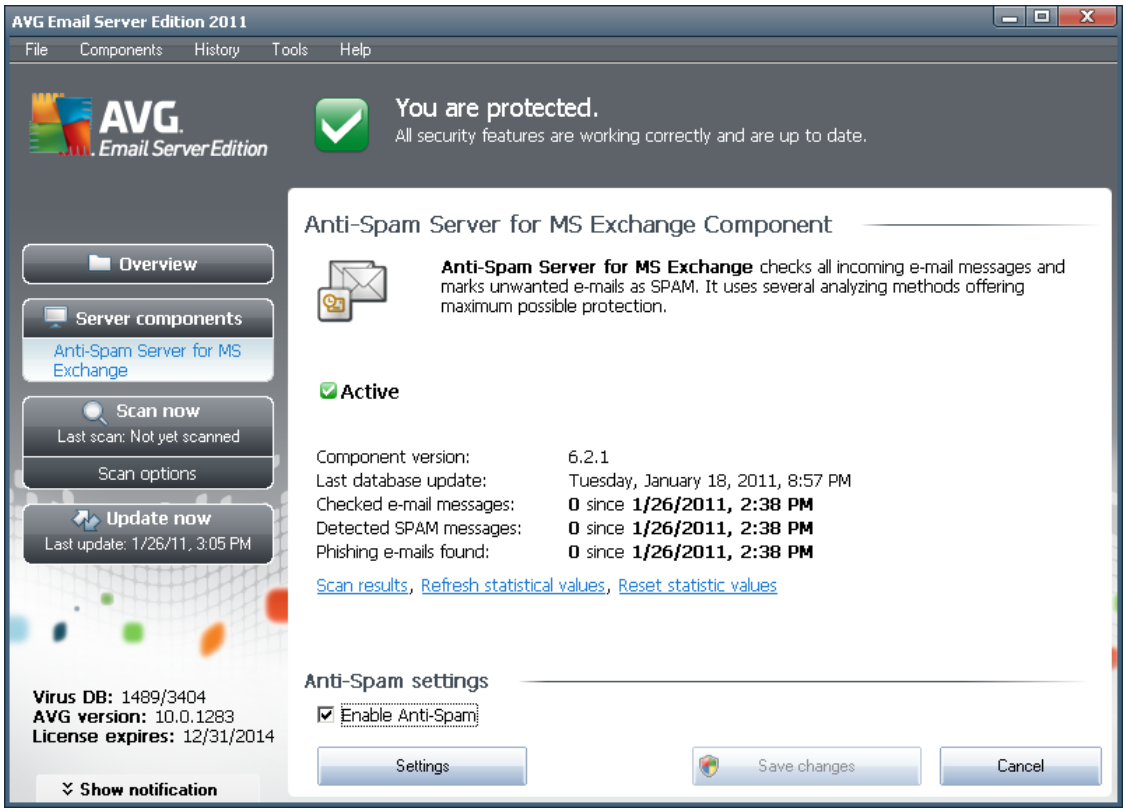
An item is removed from the list by pressing the Remove button. You can add another item to the list by pressing the ***Add...*** button. Or, you can edit an existing record by pressing the ***Edit...*** button. The following window then appears:

- In the Description field you can write a short description of the attachment to be filtered.
- In the If a mail message contains an attachment where field you can select the type of attachment (File name or MIME type). You can also choose a particular extension from the offered extensions list, or you can type the extension wildcard directly.

In the Then field you can decide whether to block the defined attachment or accept it.

7. Anti-Spam Configuration

7.1. Anti-Spam Interface

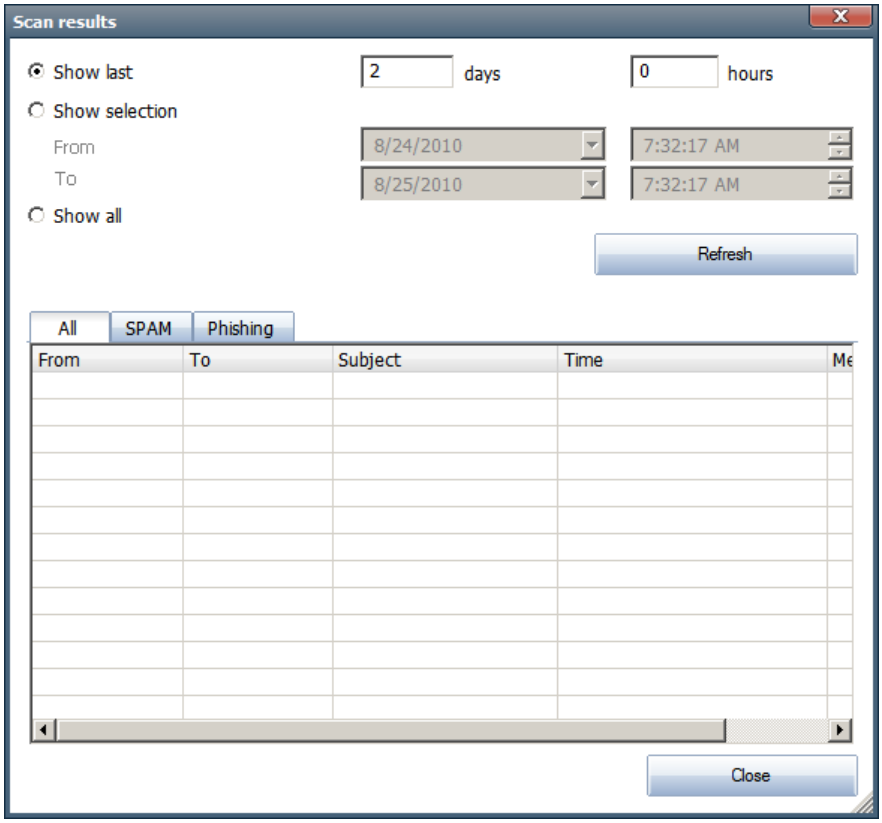

AVG Email Server Edition 2011
File
Components
History
Tools
Help
AVG. Email Server Edition
You are protected.
All security features are working correctly and are up to date.
Overview
Server components
Anti-Spam Server for MS Exchange
Scan now
Last scan: Not yet scanned
Scan options
Update now
Last update: 1/26/11, 3:05 PM
Virus DB: 1489/3404
AVG version: 10.0.1283
License expires: 12/31/2014
Show notification
Anti-Spam Server for MS Exchange Component
Anti-Spam Server for MS Exchange checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods offering maximum possible protection.
Active
Component version: 6.2.1
Last database update: Tuesday, January 18, 2011, 8:57 PM
Checked e-mail messages: 0 since 1/26/2011, 2:38 PM
Detected SPAM messages: 0 since 1/26/2011, 2:38 PM
Phishing e-mails found: 0 since 1/26/2011, 2:38 PM
Scan results, Refresh statistical values, Reset statistic values
Anti-Spam settings
Enable Anti-Spam
Settings
Save changes
Cancel

You will find the ***Anti-Spam*** server component's dialog in the ***Server Components*** section (left menu). It contains a brief information about the functionality of the server component, information on its current status (*Anti-Spam Server for MS Exchange component is active.*), and some statistics.

Available links:

- ***Scan Results***

  Opens a new dialog where you can review anti-spam scan results:



Here you can check messages detected either as a SPAM (unwanted messages) or a Phishing attempt (an effort to steal your personal data, banking details, identity etc.). By default there are displayed only results for the last two days. You can change the displayed period by amending the following options:

- ***Show last*** - insert preferred days and hours.
- ***Show selection*** - choose a custom time and date interval.
- ***Show all*** - Displays results for the whole time period.

Use ***Refresh*** button to reload the results.

- ***Refresh statistical values*** - updates stats displayed above.
- ***Reset statistical values*** - resets all the stats to zero.

The **Anti-Spam settings** section of the dialog contains a single checkbox ***Enable Anti-Spam***. Uncheck it to disable Anti-Spam protection (i. e. deactivate the whole component). Anti-Spam protection can be turned on again either using this same checkbox, or by checking similar checkbox in Anti-Spam settings.

The working buttons are as follows:

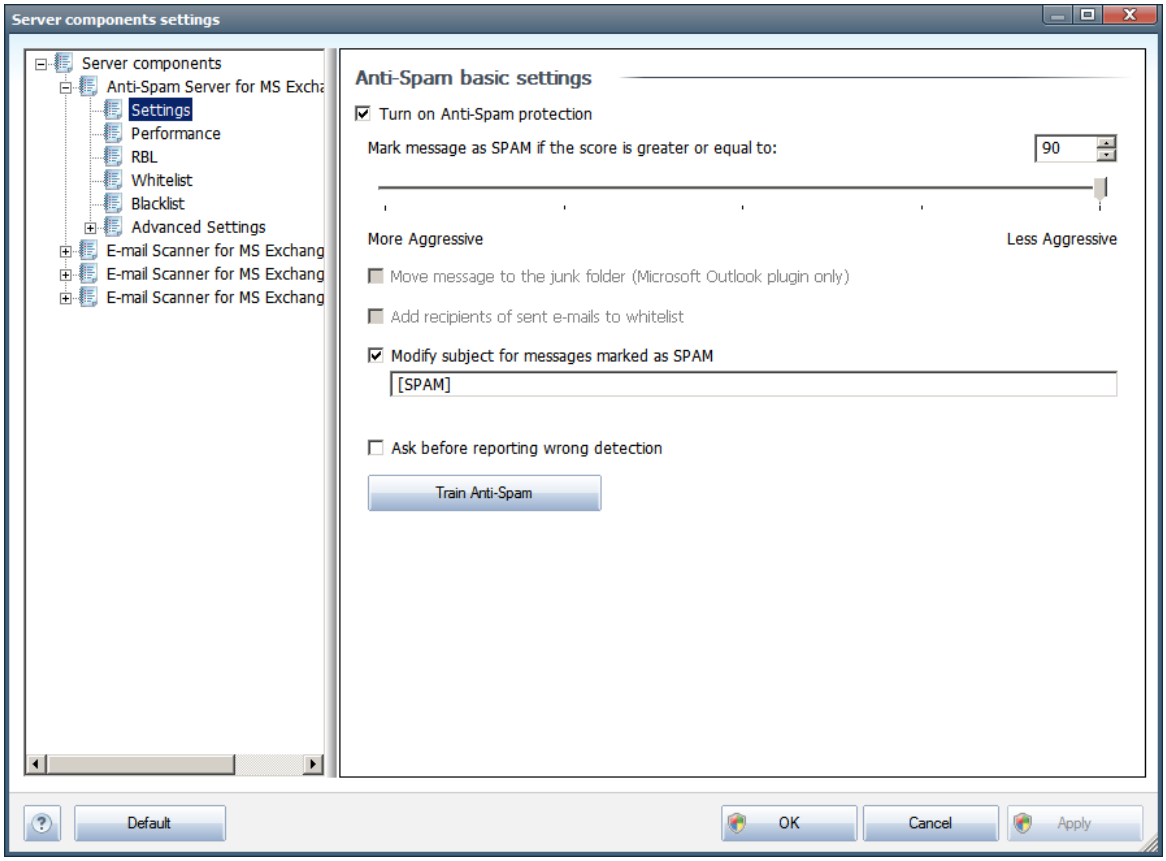
- ***Settings*** - use this button to open Anti-Spam settings.
- ***Back*** - press this button to return to the Server components overview.

7.2. Anti-Spam Principles

Spam refers to unsolicited e-mail, mostly advertising a product or service that is mass mailed to a huge number of e-mail addresses at a time, filling recipients' mail boxes. Spam does not refer to legitimate commercial e-mail for which consumers have given their consent. Spam is not only annoying, but also can often be a source of scams, viruses or offensive content.

Anti-Spam checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods to process each e-mail message, offering maximum possible protection against unwanted e-mail messages.

7.3. Anti-Spam Settings



In the ***Anti-Spam basic settings*** dialog you can check the ***Turn on Anti-Spam protection*** checkbox to allow/forbid the anti-spam scanning of e-mail communication.

In this dialog you can also select more or less aggressive scoring measures. The ***Anti-Spam*** filter assigns each message a score (*i.e. how similar the message content is to SPAM*) based on several dynamic scanning techniques. You can adjust the ***Mark message as spam if the score is greater or equal to*** setting by either typing the value (*50 to 90*) or by moving the slider left or right.

Here is a general review of the scoring threshold:

- ***Value 90*** - Most incoming e-mail messages will be delivered normally (without being marked as spam). The most easily identified spam will be filtered out, but a significant amount of spam may still be allowed through.
- ***Value 80-89*** - E-mail messages likely to be spam will be filtered out. Some non-spam messages may be incorrectly filtered as well.
- ***Value 60-79*** - Considered as a quite aggressive configuration. E-mail messages that are possibly spam will be filtered out. Non-spam messages are likely to be caught as well.
- ***Value 50-59*** - Very aggressive configuration. Non-spam e-mail messages are as likely to be caught as real spam messages. This threshold range is not recommended for normal use.

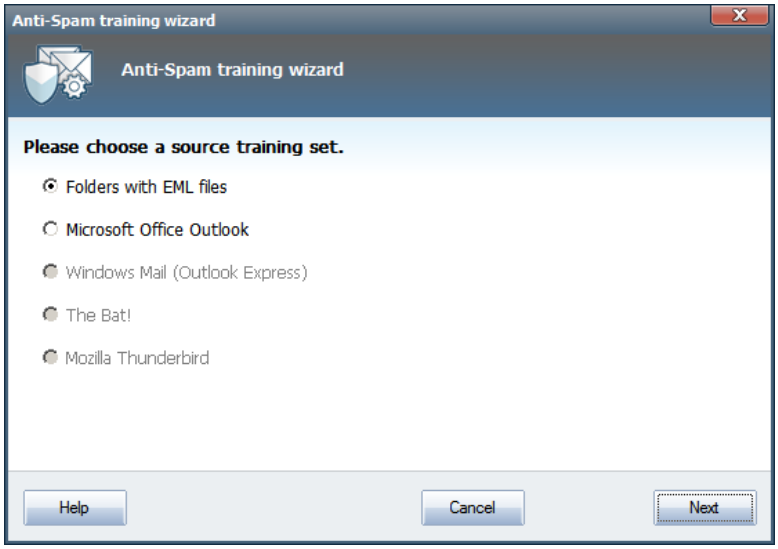
You can further define how the detected spam e-mail messages should be treated:

- ***Modify subject for messages marked as spam*** - tick this check box if you would like all messages detected as spam to be marked with a specific word or character in the e-mail subject field; the desired text can be typed in the activated text field.
- ***Ask before reporting wrong detection*** - provided that during the installation process you agreed to participate in the Product Improvement Programme - this programme helps us to collect up-to-date information on the latest threats from all participants worldwide, and in return we can improve protection for everyone - i.e. you allowed reporting of detected threats to AVG. The reporting is taken care of automatically. However, you may mark this check box to confirm you want to be asked before any detected spam gets reported to AVG to make sure the message should really be classified as spam.

Train Anti-Spam button opens the ***Anti-Spam training wizard*** described in details in the next chapter.

7.3.1. Anti-Spam Training Wizard

The first dialog of the ***Anti-Spam Training Wizard*** asks you to select the source of e-mail messages you want to use for training. Usually, you will want to use either e-mails that have been incorrectly marked as SPAM, or spam messages that have not been recognized.



There are the following options to choose from:

- ***A specific e-mail client*** - if you use one of the listed e-mail clients (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), simply select the respective option
- ***Folder with EML files*** - if you use any other e-mail program, you should first save the messages to a specific folder (in *.eml format*), or make sure that you know the location of your e-mail client message folders. Then select ***Folder with EML files***, which will enable you to locate the desired folder in the next step

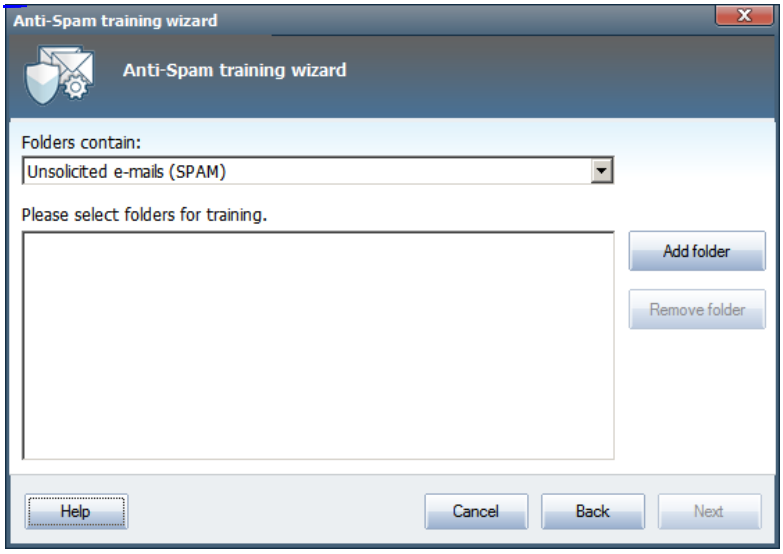
For faster and easier training process, it is a good idea to sort the e-mails in the folders beforehand, so that the folder you will use for training contains only the training messages (either wanted, or unwanted). However, it is not necessary, as you will be able to filter the e-mails later on.

Select the appropriate option and click ***Next*** to continue the wizard.

7.3.2. Select Folder with Messages

Dialog displayed in this step depends on your previous selection.

Folders with EML files



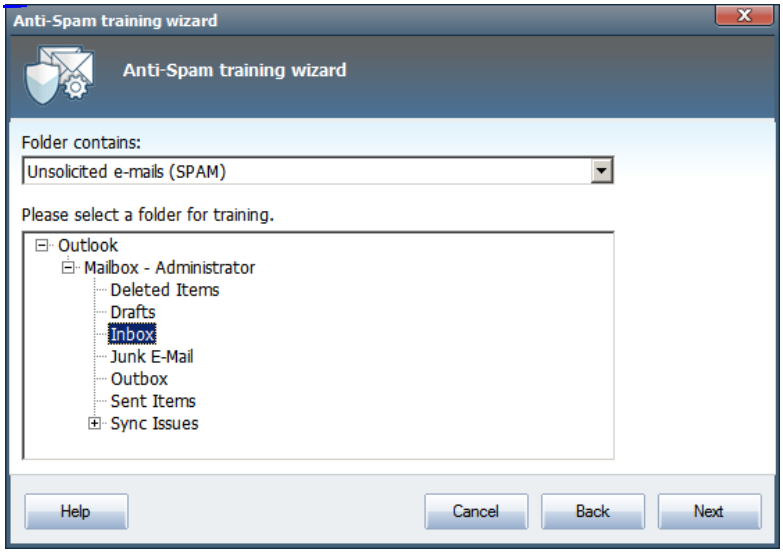
In this dialog, please select the folder with the messages you want to use for training. Press the ***Add folder*** button to locate the folder with the .eml files (*saved e-mail messages*). The selected folder will then be displayed in the dialog.

In the ***Folders contain*** drop-down menu, set one of the two options - whether the selected folder contains wanted (*HAM*), or unsolicited (*SPAM*) messages. Please note that you will be able to filter the messages in the next step, so the folder does not have to contain only training e-mails. You can also remove unwanted selected folders from the list by clicking the ***Remove folder*** button.

When done, click ***Next*** and proceed to ***Message filtering options***.

Specific e-mail client

Once you confirm one of the options, new dialog will appear.

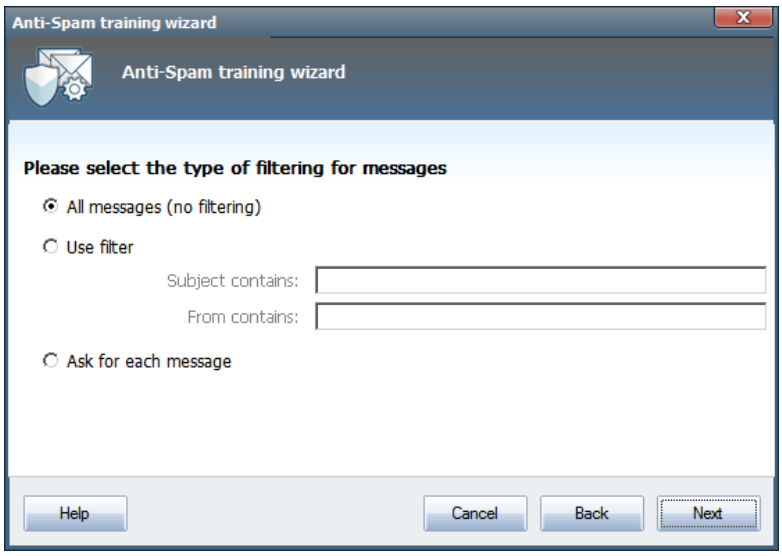


Note: *In case of Microsoft Office Outlook, you will be prompted to select the MS Office Outlook profile first.*

In the ***Folders contain*** drop-down menu, set one of the two options - whether the selected folder contains wanted (*HAM*), or unsolicited (*SPAM*) messages. Please note that you will be able to filter the messages in the next step, so the folder does not have to contain only training e-mails. A navigation tree of the selected e-mail client is already displayed in the main section of the dialog. Please locate the desired folder in the tree and highlight it with your mouse.

When done, click ***Next*** and proceed to ***Message filtering options***.

7.3.3. Message filtering options



In this dialog, you can set filtering of the e-mail messages.

If you are sure that the selected folder contains only messages you want to use for training, select the ***All messages (no filtering)*** option.

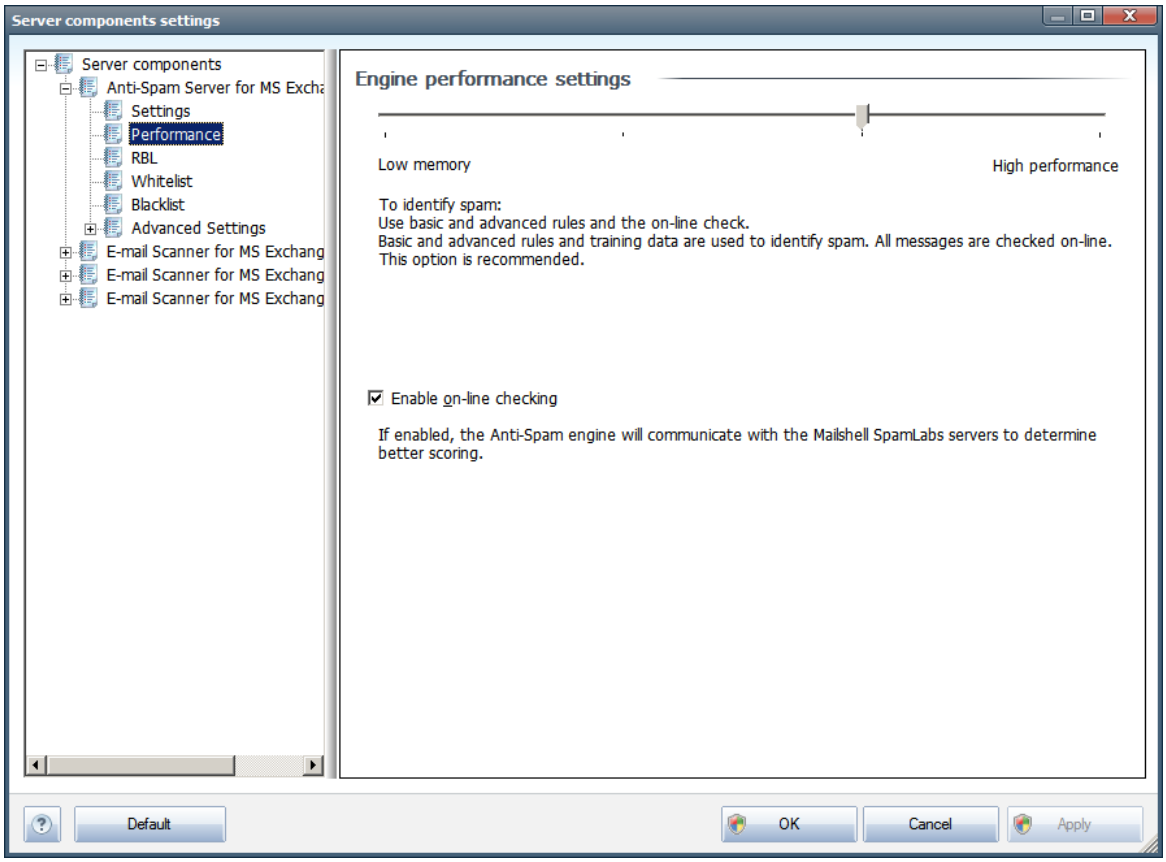
If you are unsure about the messages contained in the folder, and you want the wizard to ask you about every single message (so that you can determine whether to use it for training or not), select the ***Ask for each message*** option.

For more advanced filtering, select the ***Use filter*** option. You can fill in a word (name), part of a word, or phrase to be searched for in the e-mail subject and/or the sender's field. All messages matching exactly the entered criteria will be used for the training, without further prompting.

Attention!: *When you fill in both text fields, addresses that match just one of the two conditions will be used, too!*

When the appropriate option has been selected, click ***Next***. The following dialog will be informative only, telling you that the wizard is ready to process the messages. To start training, click the ***Next*** button again. Training will then start according to previously selected conditions.

7.4. Performance



The ***Engine performance settings*** dialog (*linked to via the* ***Performance*** *item of the*

left navigation) offers the ***Anti-Spam*** component performance settings. Move the slider left or right to change the level of scanning performance ranging between ***Low memory*** / ***High performance*** modes.

- ***Low memory*** - during the scanning process to identify spam, no rules will be used. Only training data will be used for identification. This mode is not recommended for common use, unless the computer hardware is really poor.

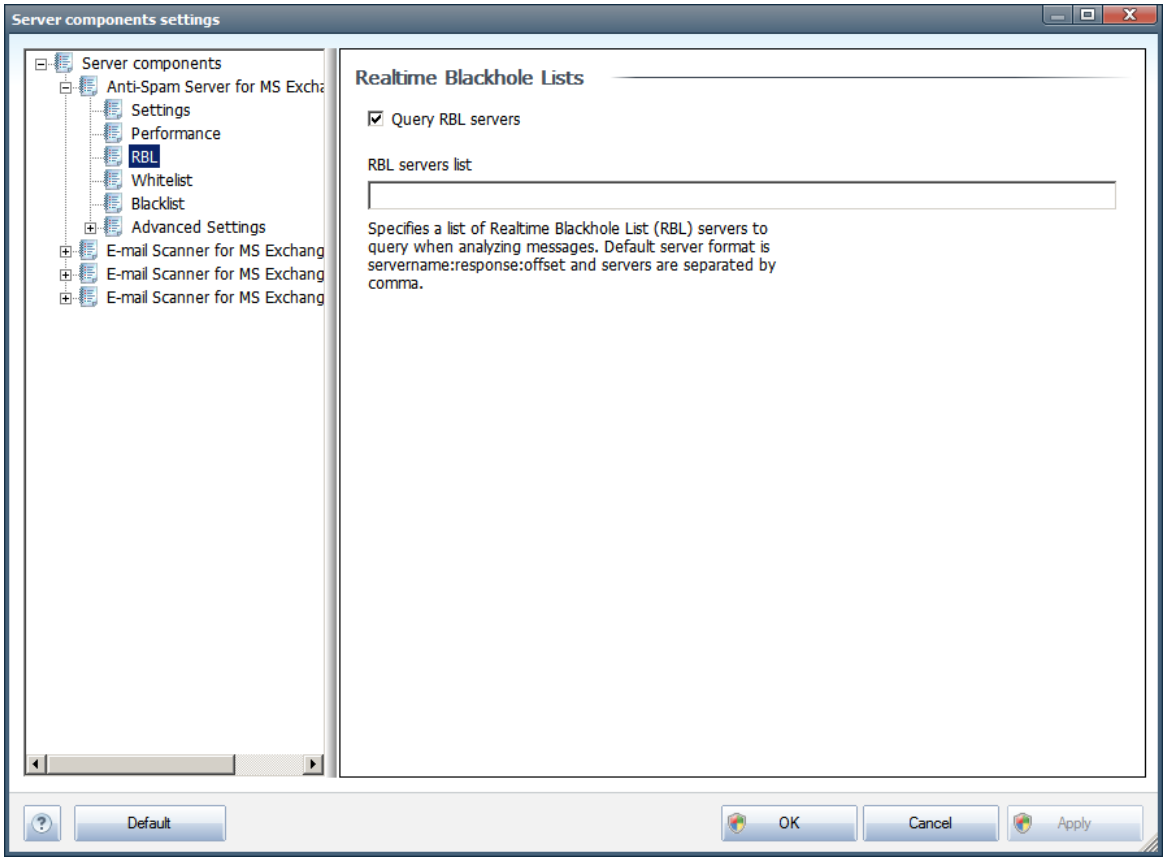
- ***High performance*** - this mode will consume large amount of memory. During the scanning process to identify spam, the following features will be used: rules and spam database cache, basic and advanced rules, spammer IP addresses and spammer databases.

The ***Enable on-line checking*** item is on by default. It results in more precise spam detection via communication with the Mailshell servers, i.e. the scanned data will be compared with Mailshell databases online.

Generally it is recommended to keep the default settings and only change them if you have a valid reason to do so. Any changes to this configuration should only be done by expert users!

7.5. RBL

The ***RBL*** item open an editing dialog called ***Realtime Blackhole Lists***:



In this dialog you can switch on/off the ***Query RBL servers*** function.

The RBL (*Realtime Blackhole List*) server is a DNS server with an extensive database of known spam senders. When this feature is switched on, all e-mail messages will be verified against the RBL server database and marked as spam if identical to any of the database entries.

The RBL servers databases contain the latest up-to-the-minute spam fingerprints, to provide the very best and most accurate spam detection. This feature is especially useful for users who receive large amounts of spam that is not being normally detected by the Anti-Spam engine.

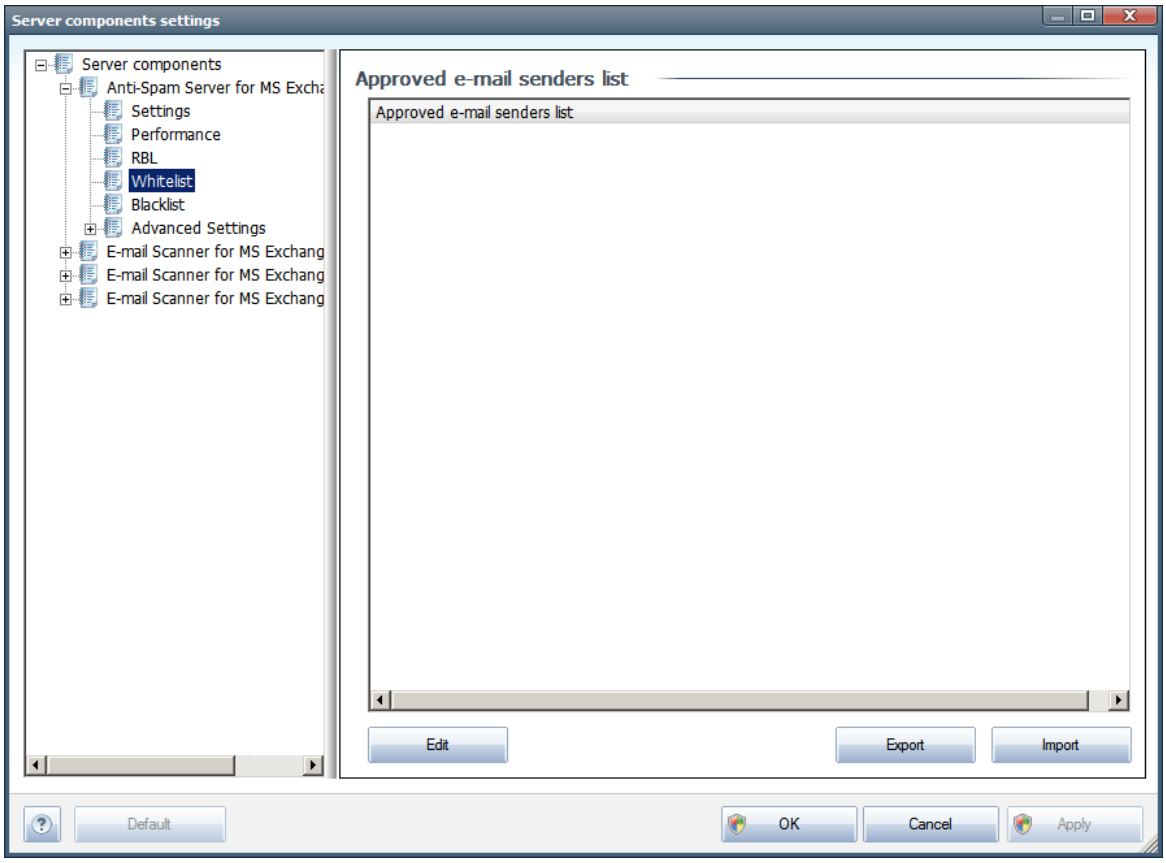
The ***RBL servers list*** allows you to define specific RBL server locations. By default, two RBL server addresses are specified. We recommend to keep the default settings unless you are an experienced user and really need to change these settings!

Note: *Enabling this feature may, on some systems and configurations, slow down the e-mail receiving process, as every single message must be verified against the RBL server database.*

No personal data is sent to the server!

7.6. Whitelist

The ***Whitelist*** item opens a dialog with a global list of approved sender e-mail addresses and domain names whose messages will never be marked as spam.



In the editing interface you can compile a list of senders that you are sure will never send you unwanted messages (spam). You can also compile a list of full domain names (e.g. *avg.com*), that you know do not generate spam messages.

Once you have such a list of senders and/or domain names prepared, you can enter them by either of the following methods: by direct entry of each e-mail address or by importing the whole list of addresses at once. The following control buttons are available:

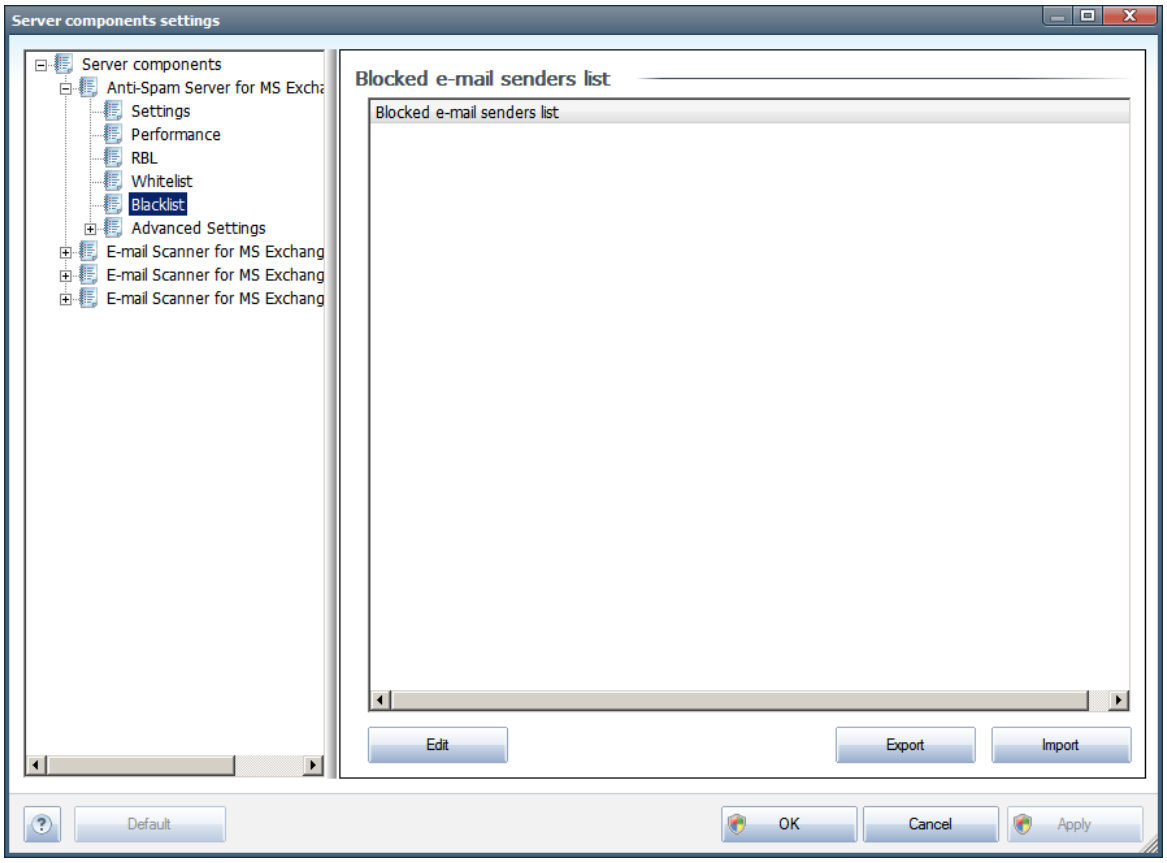
- ***Edit*** - press this button to open a dialog, where you can manually enter a list of addresses (you can also use *copy and paste*). Insert one item (sender, domain name) per line.
- ***Import*** - you can import your existing e-mail addresses by selecting this button. The input file can be a text file (in plain text format, and the content must contain only one item - address, domain name - per line), WAB file or the import

can be done from Windows Address Book or Microsoft Office Outlook.

- ***Export*** - if you decide to export the records for some purpose, you can do so by pressing this button. All records will be saved to a plain text file.

7.7. Blacklist

The ***Blacklist*** item opens a dialog with a global list of blocked sender e-mail addresses and domain names whose messages will always be marked as spam.



In the editing interface you can compile a list of senders that you expect to send you unwanted messages (spam). You can also compile a list of full domain names (e.g. *spammingcompany.com*), that you expect or receive spam messages from. All e-mail from the listed addresses/domains will be identified as spam.

Once you have such a list of senders and/or domain names prepared, you can enter them by either of the following methods: by direct entry of each e-mail address or by importing the whole list of addresses at once. The following control buttons are available:

- ***Edit*** - press this button to open a dialog, where you can manually enter a list of addresses (you can also use *copy and paste*). Insert one item (sender, domain name) per line.

- ***Import*** - you can import your existing e-mail addresses by selecting this button. The input file can be a text file (in plain text format, and the content must contain only one item - address, domain name - per line), WAB file or the import can be done from Windows Address Book or Microsoft Office Outlook.

- ***Export*** - if you decide to export the records for some purpose, you can do so by pressing this button. All records will be saved to a plain text file.

7.8. Advanced Settings

Typically it is recommended to keep the default settings and only change them if you have a valid reason to do so. Any changes to configuration should only be done by expert users!

If you still believe you need to change the Anti-Spam configuration at the very advanced level, please follow the instructions provided directly in the user interface. Generally, in each dialog you will find one single specific feature and you can edit it - its description is always included in the dialog itself:

- ***Cache*** - fingerprint, domain reputation, LegitRepute

- ***Training*** - maximum word entries, auto training threshold, weight

- ***Filtering*** - language list, country list, approved IPs, blocked IPs, blocked countries, blocked charsets, spoofed senders

- ***RBL*** - RBL servers, multihit, threshold, timeout, maximum IPs

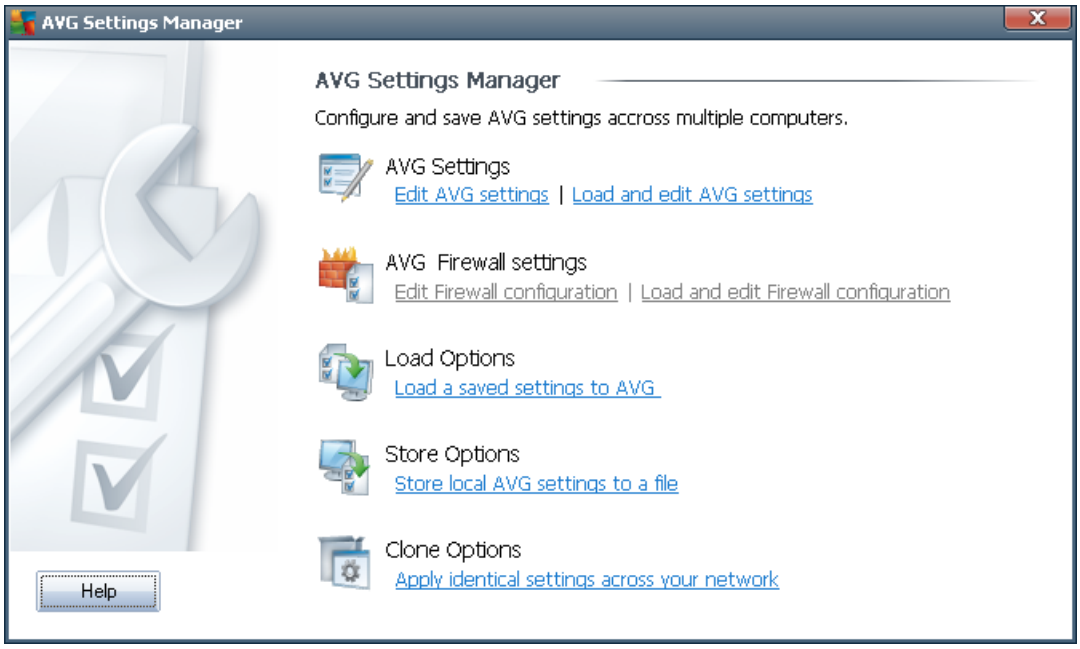
- ***Internet connection*** - timeout, proxy server, proxy server authentication

8. AVG Settings Manager

The ***AVG Settings Manager*** is a tool suitable mainly for smaller networks that allows you to copy, edit and distribute AVG configuration. The configuration can be saved to a portable device (USB flash drive etc.) and then applied manually to chosen stations.

The tool is included in the installation of AVG and available via Windows Start menu:

All Programs/AVG 2011/AVG Settings Manager


AVG Settings Manager
AVG Settings Manager
Configure and save AVG settings accross multiple computers.
AVG Settings
Edit AVG settings | Load and edit AVG settings
AVG Firewall settings
Edit Firewall configuration | Load and edit Firewall configuration
Load Options
Load a saved settings to AVG
Store Options
Store local AVG settings to a file
Clone Options
Apply identical settings across your network
Help

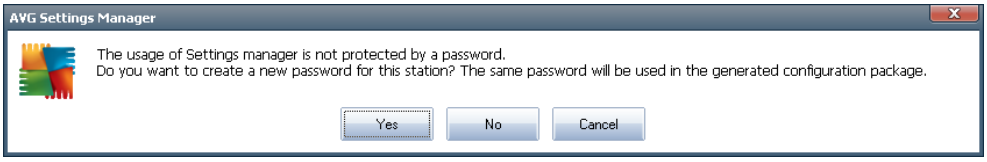
- **AVG Settings**
    - ***Edit AVG Settings*** - use this link to open dialog with advanced settings of your local AVG. All changes made here will be reflected also to the local AVG installation.
    - ***Load and edit AVG settings*** - if you already have an AVG configuration file (.pck), use this button to open it for editing. Once you confirm your changes by the ***OK*** or ***Apply*** button, the file will be replaced with the new settings!
- **AVG Firewall settings**

    This section would allow you to make changes to Firewall settings of your local AVG installation, or to edit Firewall settings in already prepared AVG configuration file (.pck). However, since your AVG Email Server Edition 2011 doesn't include the Firewall component, both links are grayed out and functionless.
- **Load Options**

- ***Load a saved settings to AVG*** - use this link to open an AVG configuration file (.pck) and apply it to the local installation of AVG.

- **Store Options**

  - ***Store local AVG settings to a file*** - use this link to save the AVG configuration file (.pck) of the local AVG installation. If you did not set a password for the Allowed actions, you may experience the following dialog:


AVG Settings Manager
The usage of Settings manager is not protected by a password.
Do you want to create a new password for this station? The same password will be used in the generated configuration package.
Yes
No
Cancel

Answer ***Yes*** if you wish to set the password for access to Allowed items now and then fill-in the required information and confirm your choice. Answer ***No*** to skip the password creation and continue to save the local AVG configuration to a file.

- **Clone Options**

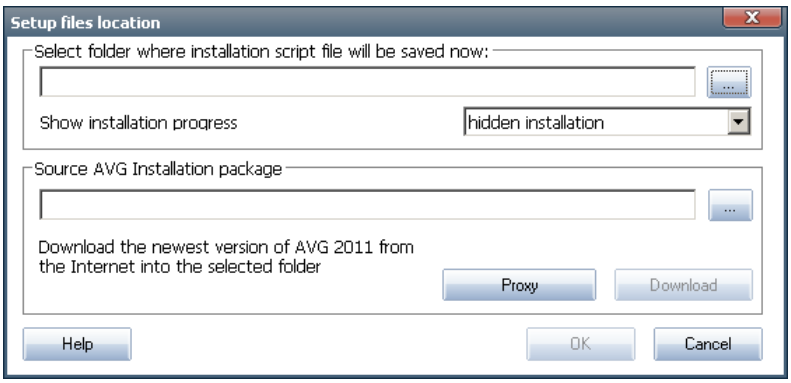
  - ***Apply identical settings across your network*** - clicking this link allows you to make a copy of the local AVG installation by creating an installation package with custom options. The clone includes most of the AVG settings with the exception of the following:

    ✓ *Language settings*

    ✓ *Sounds settings*

    ✓ *Allowed list and potentially unwanted programs exceptions of the Identity protection component.*

  To proceed first select folder where the installation script will be saved.



Then from the drop-down menu select one of the following:

- ✓ *Hidden installation* - no information will be displayed during the setup process.
- ✓ *Show installation progress only* - the installation will not require any user attention, but the progress will be fully visible.
- ✓ *Show installation wizard* - the installation will be visible and user will need to manually confirm all steps.

Use either the ***Download*** button to download the latest available AVG installation package directly from the AVG website to the selected folder or manually put the AVG installation package into that folder.

You can use the ***Proxy*** button to define a proxy server settings if your network requires this for a successful connection.

By clicking ***OK*** the cloning process begins and should shortly finish. You may also experience a dialog asking about setting password to Allowed items (see above). Once finished, there should be ***AvgSetup.bat*** available in the chosen folder along with other files. If you run the ***AvgSetup.bat*** file, it will install AVG according to the parameters chosen above.

9. FAQ and Technical Support

Should you have any problems with your AVG, either business or technical, please refer to the ***FAQ*** section of the AVG website at http://www.avg.com.

If you do not succeed in finding help this way, contact the technical support department by email. Please use the contact form accessible from the system menu via ***Help / Get help online***.